

JPL PUBLICATION 80-88

Final Report of the Autonomous Spacecraft Maintenance Study Group

Michael H. Marshall
G. David Low

(NASA-CR-164076) AUTONOMOUS SPACECRAFT
MAINTENANCE STUDY GROUP Final Report (Jet
Propulsion Lab.) 42 p HC A03/MF A01

N81-20168

CSCL 22B

Unclass

G3/18 41911



February 1, 1981

Prepared for
The Air Force Office of Scientific Research
Through an agreement with
National Aeronautics and Space Administration
by
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

JPL PUBLICATION 80-88

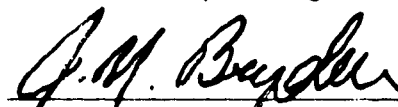
Final Report of the Autonomous Spacecraft Maintenance Study Group

Michael H. Marshall
G. David Low

Approved:



C. Carl, Study Manager



J. N. Bryden, Defense Technology
and Program Development
Office Manager

February 1, 1981

Prepared for
The Air Force Office of Scientific Research
Through an agreement with
National Aeronautics and Space Administration
by
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

The research described in this publication was carried out by the Jet Propulsion Laboratory, California Institute of Technology, and was sponsored by the Air Force Office of Scientific Research through an agreement with NASA.

Preface

As currently designed and flown, spacecraft need considerable maintenance to perform their missions. Mission readiness is jeopardized, however, because the ground support that provides the maintenance is vulnerable to both hostile action and operator errors. To address this, the Jet Propulsion Laboratory (JPL), California Institute of Technology, was commissioned in March 1980 by the Air Force Office of Scientific Research to lead a study of autonomous spacecraft maintenance (ASM). ASM is a spacecraft design that tolerates hardware and software failures and design faults, while requiring minimum ground contact to perform the mission. The study group, composed of experts from industry, academia, and NASA, was to identify critical issues related to ASM technology development and detail the infusion of this technology into future Air Force spacecraft systems. To facilitate this, three subgroups were formed: the Spacecraft System Technology Working Group, composed of spacecraft system specialists from various spacecraft suppliers; the Fault-Tolerant Technology Working Group, composed of specialists in fault-tolerant computer technology from academic and independent research institutions; and the Academic Assessment Committee, comprised of leading researchers from academic and independent research institutions.

These groups were brought together in a series of three workshops held at JPL in May, July, and August 1980, under the guidance of the Study Planning Committee. The spacecraft systems and fault-tolerant working group members presented their organizations' current capabilities in spacecraft and fault-tolerant computers, respectively, from which a state-of-the-art technical data base was established. A set of conceptual design requirements was then developed, detailing what an ASM spacecraft must do. Thus, knowing on one hand the capabilities of current spacecraft, and, on the other, the requirements for ASM, the working groups began a search for the optimum plan for the integration of ASM into spacecraft.

The major product of the Spacecraft System Technology Working Group was the Implementation Plan, which details the group's recommended approach for incorporating ASM capabilities into operational spacecraft by 1989. The Fault-Tolerant Technology Working Group and the Academic Assessment Committee together established the Research Agenda, which outlines basic research activities required to fill technological gaps.

It is hoped that the material presented here will provide guidance for the evolution of future spacecraft systems. The study participants believe that the interaction between the working groups has been synergistic, and has contributed to an increased awareness of potential technology capabilities.

Acknowledgments

Success of this study is the result of the dedication and enthusiastic participation of many individuals and their supporting organizations. The study members, gratefully acknowledged for their contributions, include:

Study Planning Committee

Mr. C. Carl, Study Manager (JPL)
Major R. Kopka (AFOSR)
Major R. Bruce (HQSD)

Mr. J. Bryden (JPL)
Lt. J. Garcia (HQSD)
Dr. G. Gilley (Aerospace Corp.)

Spacecraft System Technology Working Group

Mr. R. Draper, Chairman (JPL)
Mr. R. Bartlett (GSFC)
Mr. D. Church (LMSC)
Mr. M. Elowitz (TRW)
Mr. L. Gomberg (RCA)
Mr. T. Hoskinson (Aerospace Corp.)
Mr. D. Low (JPL)
Mr. L. Lew (RI)
Mr. M. Marshall (JPL)
Mr. R. Mullen (HAC)
Dr. A. Sabroff (TRW)
Mr. L. Scholz (RCA)

Fault-Tolerant Technology Working Group

Prof. A. Avizienis, Chairman (UCLA)
Mr. J. Goldberg (SRI International)
Dr. A. Hopkins, Jr. (Draper Labs)
Prof. D. Siewiorek (Carnegie-Mellon U.)
Dr. D. Rennels (JPL)

Academic Assessment Committee

Prof. M. Breuer (USC)
Dr. K. Daly (Draper Labs)
Prof. J. Gault (North Carolina State U.)
Dr. H. Hecht (SoHaR)
Dr. D. Hill (Battelle Columbus Labs)
Prof. G. Masson (Johns Hopkins U.)
Prof. J. Meyer (University of Michigan)
Prof. G. Metzger (University of Illinois)
Dr. M. Sievers (JPL)
Prof. K. Trivedi (Duke U.)
Mr. V. Tyree (USC Information Sciences Institute)

Abstract

This report outlines a plan to incorporate autonomous spacecraft maintenance (ASM) capabilities into Air Force spacecraft by 1989. These capabilities include the successful operation of the spacecraft without ground-operator intervention for extended periods of time. Autonomous maintenance requires extensive use of onboard fault detection, isolation, and recovery mechanisms integrated into the spacecraft within a hierarchical architecture. These mechanisms, along with a fault-tolerant data processing system (including a nonvolatile backup memory) and an autonomous navigation capability, are needed to replace the routine servicing that is presently performed by the ground system.

As part of this study, the state-of-the-art fault-handling capabilities of various spacecraft and computers are described, and a set of conceptual design requirements needed to achieve ASM are established. From these two inputs, an implementation plan describing near-term technology development needed for an ASM proof-of-concept demonstration by 1985, and a research agenda addressing long-range academic research for an advanced ASM system of the 1990s, are established.

Acronyms

AF	Air Force
AFOSR	Air Force Office of Scientific Research
ASM	autonomous spacecraft maintenance
CY	calendar year
DMSP	Defense Meteorological Satellite Program
DSCS III	Defense Satellite Communications System III
DSP	Defense Support Program
FLTSATCOM	Fleet Satellite Communications Spacecraft
FY	fiscal year
GPS	Global Positioning System
GSFC	Goddard Space Flight Center
HAC	Hughes Aircraft Company
HQSD	Headquarters, Space Division
JPL	Jet Propulsion Laboratory
LMSC	Lockheed Missiles and Space Company
LSI	large-scale integration
NASA	National Aeronautics and Space Administration
RI	Rockwell International
SRI	Stanford Research Institute
UCLA	University of California at Los Angeles
USAF	United States Air Force
USC	University of Southern California
VLSI	very-large-scale integration

Contents

Executive Summary	1
I. Introduction	1
II. State-of-the-Art Technology	1
III. The ASM-Enhanced System	2
IV. Implementation Plan	2
V. Research Agenda	2
VI. Conclusions and Recommendation	2
A. Conclusions	3
B. Recommendation	3
 Introduction	4
I. Current Space Systems	4
II. Definition of the Problem	4
III. Scope of the Study	4
 State-of-the-Art Technology	6
I. Spacecraft	6
A. Example Spacecraft	7
B. Fault-Handling Design Features of Spacecraft	8
C. Current Design Methodologies	9
II. Fault-Tolerant Computing	9
A. Onboard Spacecraft Computers	9
B. Fault-Tolerant Avionics Computers	10
C. Fault-Tolerant Commercial Computers	10
III. State-of-the-Art Technology Assessment	11
A. Spacecraft Technology Assessment	11
B. Fault-Tolerant Computing Technology Assessment	12
IV. Summary Observations	13
 The ASM-Enhanced System	14
I. Candidate Design Requirements	14
II. Impact on the Ground and Space Segments	16
III. A Hierarchical Description of the Space Segment	16

Implementation Plan	19
I. Introduction	19
A. Purpose	19
B. Goals	19
C. Approach	19
II. General Plan Description	20
III. Task Descriptions	20
A. Task 1: Existing Subsystem Redesign to ASM	20
B. Task 2: ASM System Demonstration	21
C. Task 3: Applications Research	22
D. Task 4: Advanced ASM System Development	22
E. Program Cost Estimate	22
IV. Summary	22

Research Agenda	24
I. Introduction	24
II. Research Plan	25
A. VLSI Technology	25
B. Architecture of Advanced ASM Systems	25
C. Software Fault Tolerance	26
D. Modeling and Analysis	27
E. Supporting Development	28

Conclusions and Recommendation	29
I. Conclusions	29
II. Recommendation	30

References	31
-------------------	----

Figures

1. Implementation plan outline	3
2. The space system	5
Example of a system architecture for ASM spacecraft	17
3. "Layered" architecture of fault processing	18
5. Autonomous spacecraft maintenance program	21

Tables

1. FLTSATCOM fault-handling characteristics	7
2. LEASAT fault-handling characteristics	7
3. Global Positioning System fault-handling characteristics	7
4. Defense Meteorological Satellite Program fault-handling characteristics	8
5. Multimission Modular Spacecraft fault-handling characteristics	8
6. Voyager fault-handling characteristics	8
7. ASM program resource estimate	23

Executive Summary

I. Introduction

Spacecraft are presently designed to interact with the ground-control/operations center for routine maintenance and for fault diagnosis and reconfiguration in the event of onboard problems. During periods of conflict, however, the control/operations center is vulnerable to hostile action. To continue operation during these periods, spacecraft must be capable of autonomously performing predetermined ground functions; this is accomplished by autonomous spacecraft maintenance (ASM). ASM maintains the spacecraft in a state of readiness by providing spacecraft designs that require no ground contact/interaction for onboard detection, isolation, and recovery from faults or for routine operations such as power management.

The study group was commissioned to determine a way to incorporate ASM into spacecraft. To do this, they first made a state-of-the-art technology assessment of current spacecraft systems, and then determined some general requirements for an ASM spacecraft. From this, they developed the Implementation Plan that leads to the incorporation of ASM into operational spacecraft by 1989. Included in this was an identification of the needed technologies to fill immediate gaps. To address longer-term technology issues for use in a second-generation ASM spacecraft of the 1990s, the study group also developed the Research Agenda.

II. State-of-the-Art Technology

The members of the working groups presented examples of current spacecraft and fault-tolerant computer systems,

describing their fault-handling characteristics. Examples of the spacecraft presented were: FLTSATCOM and LEASAT (communications), Global Positioning System (navigation), Defense Meteorological Satellite Program (meteorological), NASA's Multimission Modular Spacecraft (multimission), and Voyager (planetary exploration). Although each of these spacecraft perform some functions autonomously, none is capable of fully autonomous operation, mainly because this capability has never been required or specified. The fault-tolerant computers described were: Fault-Tolerant Spaceborne Computer and Building Block Fault-Tolerant Computer (spaceborne); C.mmp, Cm*, and C.vmp (commercial); and Software Implemented Fault-Tolerance and Fault-Tolerant Multiprocessor (commercial aviation). Of the fault-tolerant computers presented, none is operational yet, and only the Fault-Tolerant Spaceborne Computer and Building Block Fault-Tolerant Computer will be applicable to spacecraft systems. The others, however, provided examples of design methodologies and techniques that may be applicable to spaceborne computers.

Each of the spacecraft that was presented required interaction with the ground system for normal operations management, as well as fault diagnosis and recovery. This interaction was needed for such things as power management, housekeeping, navigation corrections, and any abnormalities that occurred. Having the spacecraft rely on the control/operations center makes the overall space system as vulnerable as the control/operations center. It also creates a long "down time" wherever a fault occurs, because the fault must be diagnosed and reconfiguration commands must be developed by the control/operations center. This vulnerability and down time can be reduced by shifting the management of routine

operations and fault handling from the ground to the spacecraft (i.e., the spacecraft performs them autonomously).

Thus, the need for ASM is recognized; furthermore, the study group believes that the technology available in today's spacecraft systems is a good foundation from which to proceed to ASM.

III. The ASM-Enhanced System

The impact of ASM on future Air Force spacecraft is based upon an analysis of the current system's ability to meet the candidate design requirements formulated by the study group. In summary, these ASM conceptual design requirements are:

- (1) The ASM spacecraft shall operate without ground intervention for up to 60 days with no performance degradation, and up to 6 months with degraded, but acceptable, performance. (The actual periods of autonomy may vary with different mission applications; however, the participants felt that these were worthwhile goals for this study.)
- (2) ASM shall not reduce the spacecrafts' performance or design lifetime.
- (3) The ground segment shall always be able to override ASM actions and interrogate the spacecraft for fault-management data (audit trails).

Satisfying these design requirements implies the movement of routine maintenance and operations from the ground segment to the space segment. The control/operations center will assume a supervisory role, potentially less complex, while the space segment will become more complex. The resulting benefits of ASM would then include: (1) reduced system vulnerability because the spacecraft is no longer dependent upon the control/operations center and (2) faster recovery from failures (seconds instead of hours or possibly days).

The impact of ASM on spacecraft design is expected to be evolutionary. Traditional subsystems are expected to be augmented by two new subsystems: a fault-tolerant data processing subsystem with nonvolatile back-up memory, and an autonomous navigation subsystem.

The system architecture is expected to possess a "layered" fault-protection scheme, enabling fault containment at the lowest possible level to minimize subsystem interdependencies. In this scheme, individual subsystems, under system control, will be required to diagnose local failures and take corrective action. The system will be required to diagnose and correct ambiguous failures within the subsystem interfaces and ASM mechanisms themselves, as well as to judiciously allocate the system resources.

IV. Implementation Plan

The Implementation Plan focuses on near-term industrial technology development and, most importantly, the earliest possible system-level proof-of-concept demonstration (1985) to support a 1989 launch. The plan stresses delivery of "product" in a steady stream from subsystems to a complete system for the System Program Offices' consideration and introduction into flight programs.

As shown in Fig. 1, the Implementation Plan consists of four major tasks. These are: (1) redesign of existing subsystems to characterize and demonstrate ASM capabilities; (2) design, develop, and test an ASM system demonstration breadboard to show that ASM is a viable concept; (3) perform applications research required to develop an autonomous navigation capability and a fault-tolerant data processing capability to fill existing technology gaps; and (4) basic research needed to develop a second-generation ASM system for the 1990s. A section of this report, "Research Agenda," elaborates upon Task 4.

A budgetary resource estimate for the proposed ASM program is \$36.4M (FY80 dollars) over five years. For several reasons, this figure should be considered only an estimate. First, the cost of developing the new technology is not well known. Second, a specific mission application has not been assumed, and so candidate spacecraft could not be assumed. Finally, substantiating data was not provided by the industrial participants. For these reasons, a more definitive cost study should be performed in the initial phase of the activity.

V. Research Agenda

The Research Agenda proposes basic research that is a synergistic part of the ASM program. Future ASM development activities are focused on five areas: (1) very-large-scale integration (VLSI) technology, which includes self-testing VLSI and on-chip redundancy; (2) system architecture, which addresses spacecraft organizational issues, architectural developments, and advanced system studies; (3) software fault-tolerance, consisting of system partitioning and interface definition, self-checking flight software, and fault-tolerant software; (4) modeling and analysis, comprised of experimental testing, statistical modeling, and functional description, modeling, and verification; and (5) supporting developments needed to formulate an ASM data base, and to build an ASM spacecraft laboratory.

VI. Conclusions and Recommendations

The following conclusions and recommendation are those of the study group participants, resulting from analysis of the material developed during the workshops.

A. Conclusions

- (1) ASM, fully implemented, would reduce space system vulnerability by eliminating spacecraft dependence on the control/operations center for up to 6 months at a time.
- (2) The ASM capability need not impose operational constraints on the system user; it must be "transparent" to the user during normal system operations.
- (3) ASM would require a change in the conduct of operations and control, from dependence on a man in the loop to dependence on machines for fault handling and routine maintenance operations.
- (4) ASM would increase the spacecraft complexity, therefore, new methods for specifying, testing, and validating ASM-enhanced spacecraft are needed.
- (5) A more effective means of transferring technology from research to applications programs would be required so that spacecraft problems could be solved with the latest available technology.
- (6) New technology developments would be required: needed are a highly reliable fault-tolerant data processing system with nonvolatile backup memory to enable autonomous maintenance, and an autonomous navigation capability to enable independence of routine ground operations.
- (7) ASM would be a phased program; spacecraft would not instantly become totally autonomous. The pace of ASM development would depend on the resources, technology, and chosen program applications that are available. A strong corporate commitment to ASM by the Air Force, along with a willingness by industry to assimilate ASM, would be required to make ASM successful.
- (8) Confidence in ASM must be instilled by creation of a systematic modeling, analysis, and demonstration program.
- (9) Although considerable technology developments are necessary, no requirements for technology breakthroughs have been identified.
- (10) In the opinion of the study group, ASM is a viable concept.

B. Recommendation

The study group recommends that the ASM research and technology development activities, as outlined in the Implementation Plan and Research Agenda sections of this report, be initiated as soon as possible. This would enable the earliest possible spacecraft system-level proof-of-concept demonstration of ASM.

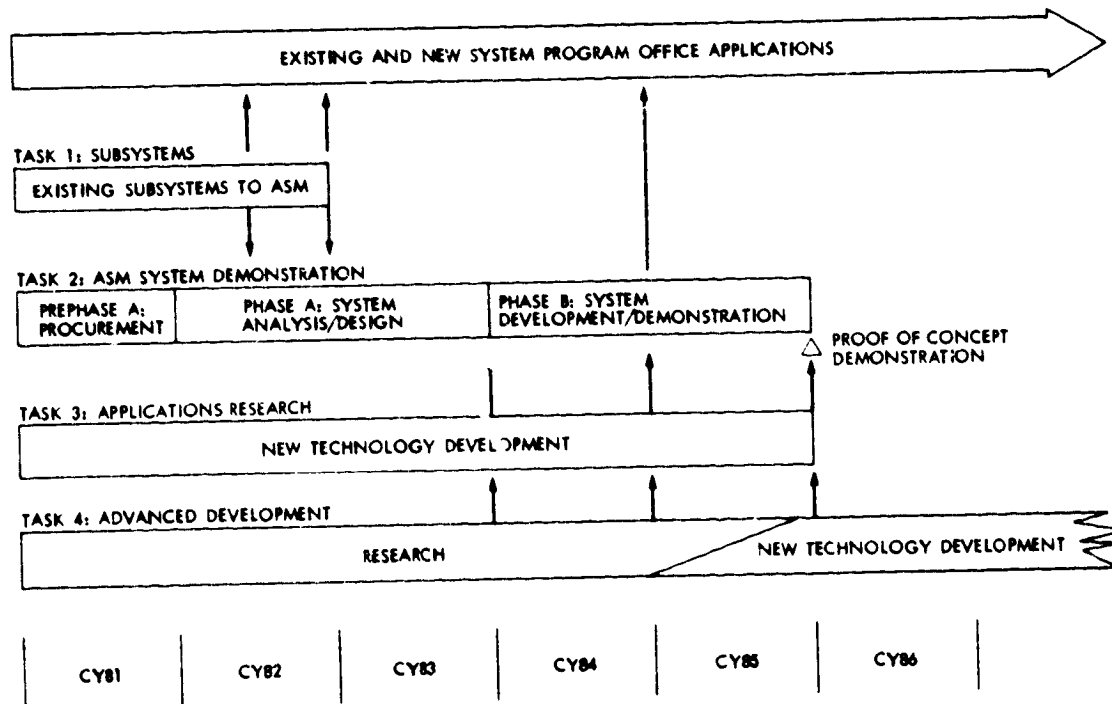


Fig. 1. Implementation plan outline

Introduction

Currently, when certain critical failure states are detected, spacecraft usually enter a "safe-hold" mode; in this mode, operations are suspended and ground intervention in the form of reconfiguration commands is required to restore normal operations. Spacecraft are also not presently designed to autonomously recover from design faults, software failures, or changing environmental conditions.

Autonomous spacecraft maintenance is characterized by:

- (1) Spacecraft design that tolerates hardware and software failures and design faults.
- (2) Spacecraft design that requires - for extended periods of time - virtually no ground contact/interaction for onboard detection, isolation, and recovery of faults, or routine maintenance functions.

For the most part, such capabilities have been beyond the state of the art of spacecraft systems. This study group has been commissioned by the Air Force to address these issues, and to detail a plan leading to the incorporation of ASM into operational spacecraft by 1989.

I. Current Space Systems

The space system is composed of the space segment and the ground segment, as illustrated in Fig. 2. For this study, the

space segment consists of only the spacecraft, while the ground segment consists of three separate entities: data processing stations, communications centers, and a control/operations center. The data processing stations and the communications centers may be numerous and are payload-data users only, whereas the control/operations center is nonredundant and is responsible for the overall management of the spacecraft.

II. Definition of the Problem

It can be seen that the loss of any single data processing station or communications center will not jeopardize the space segment; on the other hand, the loss of the control/operations center may eventually render the entire space system ineffective. The dependence of the spacecraft on the control/operations center and the vulnerability of the center to hostile action and operator error are the concerns of this study.

III. Scope of the Study

Spacecraft autonomy involves several elements: autonomous spacecraft maintenance, autonomous mission sequencing and control, autonomous navigation, and autonomous payload data processing. To have a completely autonomous spacecraft, all of these elements would have to be included. This study, however, was to address only the spacecraft maintenance

(spacecraft "health and welfare") aspect of autonomy. This includes the maintenance of satisfactory system performance in the presence of internal faults, and the movement of routine maintenance functions from the ground station to the spacecraft. It is assumed that other studies will address the other elements of autonomy. With this assumption in mind, the following topics were addressed:

- (1) The state of the art of ASM in spacecraft design.
- (2) An ASM design methodology.

- (3) An implementation plan leading to the demonstration of ASM concepts.
- (4) Research areas applicable to ASM.
- (5) A basic research agenda that supports the development of ASM.

These topics and their key results are discussed in the sections that follow.

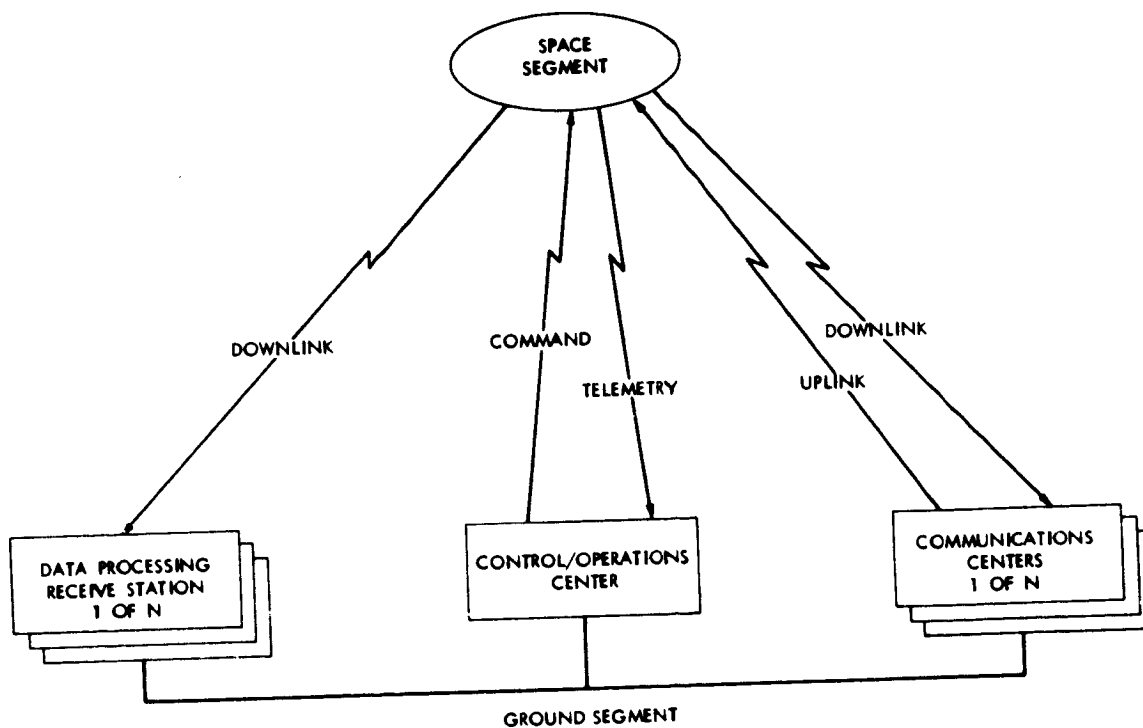


Fig. 2. The space system

State-of-the-Art Technology

The members of the Spacecraft System Technology and Fault-Tolerant Technology Working Groups presented descriptions of the fault-handling characteristics of existing spacecraft and fault-tolerant computer systems. These were representative of successful systems designed to operate within specific environments: the spacecraft systems for the space environment, and the computer systems (to date) within laboratory environments. In this section, a summary of the current capabilities of the spacecraft and fault-tolerant computer systems is given, followed by an assessment of their relevance to ASM.

I. Spacecraft

Air Force satellites can be categorized into four mission classes: communications, navigation, meteorological, and surveillance. During the workshops, satellites from each of the classes except surveillance were presented. Because surveillance satellites were classified, no detailed information was solicited. Additionally, presentations were given describing some of the planetary exploration spacecraft.

The members of the Spacecraft System Technology Working Group were chosen because of their expertise in the

subject field and because of their affiliated organization's experience as a supplier of Air Force spacecraft for one or more of the mission classes. Each member described examples of current spacecraft, explaining its design methodology relating to fault handling. Numerous systems and subsystems were described by the participants; the systems presented in this section are examples only, representing the different mission classes. It is not being suggested that these spacecraft are leading candidates for their mission application. Such an assessment was not a part of the study. The fault-handling characteristics of the following spacecraft will be described:

Mission class	Example spacecraft
Communications	FLTSATCOM, LEASAT
Navigation	Global Positioning System
Meteorological	Defense Meteorological Satellite Program
Multimission	Multimission Modular Spacecraft
Planetary exploration	Voyager

A. Example Spacecraft

1. **Communications spacecraft.** FLTSATCOM is a 3-axis stabilized, 23-channel communications satellite. It flies in a geosynchronous orbit and has a 5-year design life. Four of these spacecraft are operational; the first was launched on February 9, 1978. Its fault-handling characteristics are given in Table 1.

Table 1. FLTSATCOM fault-handling characteristics

Fault-tolerant attribute	Description
Onboard hardware	Reliability achieved by redundant components Cross-strapping Onboard switching to "safe-hold" mode Undervoltage detection resulting in automatic load shed Battery cell monitor and switching Command receiver toggle
Onboard software	None
Ground assisted	Allow ground intervention for failure analysis and switching Redundancy management on ground Ground override capability

LEASAT is a spin-stabilized geosynchronous communications satellite designated as a functional follow-on to FLTSATCOM, with a design life of 10 years. Four satellites will be shuttle-launched beginning in 1984. These satellites' fault-handling characteristics are given in Table 2.

Table 2. LEASAT fault-handling characteristics

Fault-tolerant attribute	Description
Onboard hardware	Automatic transfer to rate-hold mode in event of loss of sensor Automatically activates redundant control electronics/motor driver and motor in event of loss of despin control No single-point failures in thruster operations Automatic fault detection and ground alerting Redundant elements to unit level Receiver time out Watch dog timers
Onboard software	None
Ground assisted	Allow ground intervention for failure analysis and switching Redundant switching for battery charge rates and battery reconditioning Redundancy management on ground

2. **Navigation spacecraft.** The Global Positioning System (GPS) satellite is a 3-axis stabilized, semisynchronous (12-hour orbit) navigation satellite. It will enable a user to accurately determine his position, velocity, and time. When fully operational, there will be 18 satellites on orbit. To date six have been launched, the first on February 22, 1977. Each satellite is designed for a mean mission duration of 5 years; the fault-handling characteristics are given in Table 3.

Table 3. Global Positioning System fault-handling characteristics

Fault-tolerant attribute	Description
Onboard hardware	Full redundancy except where impractical (e.g., structure) Multiple redundancy in critical subassemblies (e.g., triply redundant atomic clocks) Automatic detection and isolation Electrical shorts, attitude loss handled by load shedding Jet runaway handled by watchdog logic Automatic detection and correction at unit level for system performance degradation failures Earth sensor Control Electronics Assembly power supplies Masking of solar array system performance degradation failures Automatic Sun reacquisition from eclipse
Onboard software	No spacecraft bus software
Ground assisted	Allow ground intervention for failure analysis and switching Redundancy management on ground Battery reconditioning Routine health and status monitoring Ephemeris and time update Magnetic momentum dump

3. **Meteorological spacecraft.** Defense Meteorological Satellite Program (DMSP) Block 5D spacecraft are 3-axis stabilized and operate in a Sun-synchronous polar orbit at 830 km (450 nmi). The Block 5D spacecraft have a 2-year design life; the first was launched September 11, 1976. The fault-handling characteristics of these satellites are given in Table 4.

4. **Multimission spacecraft.** The Multimission Modular Spacecraft is 3-axis stabilized and can be used for various mission classes. It can be used in orbital altitudes from low-Earth to geosynchronous. The first launch was February 14, 1980. It has a 2-year mission lifetime, and is capable of being resupplied by the shuttle. Its fault-handling characteristics are given in Table 5.

Table 4. Defense Meteorological Satellite Program fault-handling characteristics

Fault-tolerant attribute	Description
Onboard hardware	Hardware watchdog timer requires periodic response, protects against loss of power and clock or system lock-up ①
	Hardware testing of parity, illegal instructions, and memory addresses (computer self-tests)
	Physical and functional redundancy in subsystems
	Hardware detection/switching in power subsystem
Onboard software	Redundant central processing units
	Protective software in power subsystem
	Solar array drive control
	Battery state of charge, low voltage, temperature checks
	Load shedding in event of fault
Ground assisted	Software response to errors tested in ① above
	Spare memory with special software packages to anticipate recovery after memory failures
	Detection/switching in subsystems other than power
	Allow ground intervention for failure analysis and switching
	Special onboard processor test; memory patterns, diagnostic instruction test
	Reprogram computers
	Data trend analysis

5. Planetary exploration spacecraft. The two 3-axis stabilized Voyager spacecraft, launched August 20 and September 5, 1977, are designed to explore the planets Jupiter and Saturn. Each spacecraft was designed for a 4-year mission lifetime, although each has enough expendables for possible extended missions. Table 6 lists Voyager's fault-handling characteristics.

B. Fault-Handling Design Features Of Spacecraft

Several observations can be made from the fault-handling characteristics of the spacecraft presented. The spacecraft typically employ block and functional redundancy for high reliability, as well as watchdog timers, cross-strapping, and switching networks for fault protection and self-preservation. In general, there are no credible single-point failures. The ground-assisted features include such capabilities as ephemeris and time updates, trend analysis, and mission reconfiguration. Redundancy management is done mostly on the ground, and in all cases the ground has an override capability.

Block redundancy employs complete, identical, extra components that can take over in the event of a component

Table 5. Multimission Modular Spacecraft fault-handling characteristics

Fault-tolerant attribute	Description
Onboard hardware	Block redundancy
	No credible single-point failures in spacecraft bus
Onboard software	Computer failure detections (watchdog timers) in the attitude control, communications, and power modules; reconfigures spacecraft to power safe Sun-pointing mode using analog backup system
	Undervoltage detection and safing
Ground assisted	Battery state-of-charge calculations
	Computer self-test
	Spacecraft off-pointing detection and safing
	Telemetry data quality checks
	Internal validity checks for attitude determination and control software
	Monitor health and safety of predetermined payload instruments with onboard safing actions
	Allow ground intervention for failure analysis and switching
	Power regulator failure detection and corrective action
	Redundancy management on ground

Table 6. Voyager fault-handling characteristics

Fault-tolerant attribute	Description
Onboard hardware	Overtemperature protection for payload instruments
	No significant single-point failures
	Block and functional redundancy
	Computer self-test
	Nonvolatile memory for Computer Command Subsystem and Attitude and Articulation Control Subsystem
	Undervoltage protection
	Parity and code checks
Onboard software	Restores command link
	Switches processors
	Switches power elements
	Switches Sun/star sensors
	Switches thrusters/plumbing
	Reprogrammable
	Event timing and event counting
	Retry for some data transmission errors
Ground assisted	Block parity validation of command sequences
	Switching of redundant components with noncatastrophic failure modes
	Alternate operating modes
	Trend analysis and calibrations

failure. There are several levels at which block redundancy can be applied. In ascending order these are the element, functional unit, functional string, subsystem, and system levels.

Functional redundancy, on the other hand, does not employ identical components, but instead performs nearly the same functions using alternate system or subsystem configurations, typically controlled from the ground. Functional redundancy has an advantage over block redundancy in that it helps avoid systematic design errors; however, it generally does not possess equal performance capability.

In the event of a failure, the operating philosophy for the spacecraft systems has been to rely on ground interaction to restore successful operations. This has given rise to the safehold mode in which the spacecraft is autonomously switched to a benign state until ground interactions restore operation. The ground action typically involves fault detection through analysis, commanded switching to isolate the defective element, and finally recovery procedures through reconfiguration of available resources.

C. Current Design Methodologies

Methodologies have been defined to include procurement/management policies and design/development procedures. The procurement/management policies structure the development process through the use of formalized management reports, design reviews, and audits. Design/development procedures refer to the collective set of design tools and test and validation procedures that are employed during the development process.

Design tools are employed to evaluate the adequacy of a proposed design prior to a commitment for fabrication. Such tools include simulation, emulation, and reliability analysis techniques (defined by MIL-HDBK-217). Testing procedures strive to show that the spacecraft operates per the design intent; they should identify faulty components and errors in manufacturing. Validation programs, on the other hand, strive to insure the agreement of the system realization with the system specification. This includes validation of performance, reliability, and environmental requirements.

II. Fault-Tolerant Computing

An assessment of the state of the art in fault-tolerant computing was undertaken as part of the ASM study for two important reasons. First, it is a technology that has been under investigation for over twenty years, and that has resulted in the development of several autonomously maintained systems (e.g. self-repairing computer systems). Second, it appears that

onboard fault-tolerant computers will be required to act as the automated repairman for ASM spacecraft.

A number of fault-tolerant computers have already been constructed and used. The largest application is in telephone switching systems. Most modern switching offices are autonomously maintained systems. The resident computer is capable of detecting faults within itself and in surrounding equipment, replacing the faulty equipment, and continuing normal service (Ref. 1). Computers with varying degrees of autonomous self-repair have been used in other commercial applications. Examples are the Pluribus Multiprocessor for communications systems, and the Tandem Computer Systems often used for financial transactions (Ref. 2). In aerospace systems, examples of fault-tolerant computing can be found in commercial airplanes, the Space Shuttle, and in the Saturn V guidance computer (Ref. 3). Thus there exists a large body of design experience in the development of fault-tolerant (i.e., autonomously self-maintained) computing systems for a variety of applications.

Although two breadboard systems have been constructed and tested, and a third is under development, fault-tolerant computing has not been used on current spacecraft. Two goals of the Fault Tolerant Technology Working Group were to provide a state-of-the-art assessment of fault-tolerant computing to the spacecraft systems technologists, and to evaluate problems and prospects for employing fault-tolerant computing in spacecraft flight systems. Each member of the working group is actively involved in the development of a state-of-the-art, fault-tolerant computing system, and each made presentations on their systems.

Seven fault-tolerant computing systems were presented. They are categorized into three groups: (1) onboard spacecraft computers, (2) avionics computers, and (3) commercial computers.

A. Onboard Spacecraft Computers

Two computer systems were presented, the Fault-Tolerant Spaceborne Computer and the Building Block Fault-Tolerant Computer.

1. Fault-Tolerant Spaceborne Computer. The Fault-Tolerant Spaceborne Computer is a general-purpose computer, designed to Air Force specifications of high throughput and a 95% probability of surviving (unattended and without degradation of performance) for 5 to 7 years. This machine is capable of self-reconfiguration and resumption of computations following internal component failures, power transients, and radiation events.

The Fault-Tolerant Spaceborne Computer is in an advanced state of development. A laboratory breadboard has been constructed and the fault-tolerance features verified by experimental testing (e.g., insertion of faults and verifying proper recovery). The machine is based on complementary metal-oxide semiconductor—silicon on sapphire LSI technology. It is not available for flight use due to an inability to obtain radiation-hardened (1000 gate/chip) integrated circuits (Ref. 4).

2. Building Block Fault-Tolerant Computer. The Building Block Fault-Tolerant Computer is a fault-tolerant distributed computer system architecture. It is aimed at spacecraft systems that employ a large number of microcomputers embedded in various subsystems, and is an outgrowth of the Unified Data System architecture developed at JPL (Ref. 5). This architecture uses a small set of standard building block circuits that allow existing microprocessors and memories to be connected together into fault-tolerant distributed computer systems. The building blocks connect the central processing unit and the random access memory to form self-checking computer modules that can detect their own internal faults during normal operation. The self-checking computer modules contain interfaces to a set of redundant intercommunication buses and can be connected into a network in which spare computers are employed for fault recovery.

A breadboard of the Building Block Fault-Tolerant Computer is currently being developed, and it is expected that it will be completed and verified in 1982. Flight availability will require the subsequent development of two VLSI and four LSI integrated circuits, and will take an additional two or three years. The problem of obtaining radiation hard parts is common to both the Fault-Tolerant Spaceborne Computer and the Building Block Fault-Tolerant Computer programs.

B. Fault-Tolerant Avionics Computers

Two avionics computers were presented. These machines have been developed by NASA for control of future fuel-efficient aircraft that will be dynamically unstable. Extremely high reliability is required since lives may depend on correct computer operation. Thus a reliability of 0.99999999 is required for every 10-hour flight mission. These avionics computers are not directly applicable to spacecraft. Weight, power, and volume greatly exceed what can be supported by a spacecraft. They are also designed to allow human maintenance after every 10-hour flight when the plane is on the ground—a condition not experienced by spacecraft.

The two avionics computers are designated Fault-Tolerant Multiprocessor and Software Implemented Fault Tolerance.

Both have been developed as breadboard systems and are currently under test. Though not immediately applicable to spacecraft, many of the techniques and insights developed in their design will be applicable to long-term research into future ASM systems. These machines are summarized below.

1. Fault-Tolerant Multiprocessor. The Fault-Tolerant Multiprocessor is intended for use as one of at least two central computers in a redundant distributed digital system designed to serve as a highly survivable avionics system. The design is based on independent processor-cache memory modules and common memory modules that communicate via redundant serial buses. All information processing and transmission is conducted in triplicate so that local voters in each module can correct errors. Modules can be retired and/or reassigned in any configuration. Reconfiguration is carried out routinely from second to second to search for latent faults in the voting and reconfiguration elements. Job assignments are all made on a floating basis, so that any processor triad is eligible to execute any job step. The core software in the Fault-Tolerant Multiprocessor will handle all fault detection, diagnosis, and recovery in such a way that applications programs do not need to be involved (Ref. 6).

2. Software Implemented Fault Tolerance. Software Implemented Fault Tolerance is an ultrareliable computer for critical aircraft control applications that achieves fault tolerance by the replication of tasks among processing units. The main processing units are off-the-shelf minicomputers. Fault isolation is achieved by using an individually-buffered, serial data link between each processor pair for all processors. Error detection and analysis and system reconfiguration are performed by software. Iterative tasks are redundantly executed, and the results of each iteration are voted upon before being used. Thus, any single failure in a processing unit or bus can be tolerated with triplication or quintuplication of tasks, and subsequent failures can be tolerated after reconfiguration. The Software Implemented Fault Tolerance software is highly structured and is formally specified using the SRI-developed SPECIAL language (Ref. 7).

C. Fault-Tolerant Commercial Computers

Three fault-tolerant computing projects at Carnegie Mellon University were presented. These systems use DEC minicomputers and are aimed at commercial applications. Though not directly applicable to spacecraft systems, some of the insights gained in their design are applicable to ASM research. These machines, designated C.mmp, Cm*, and C.vmp, are summarized below.

1. C.mmp, a multiminiprocessor. C.mmp is a canonical multiprocessor system with a 16 × 16 crosspoint switch. Up to

16 DEC PDP-11/40 processors may be connected to the processor ports on the switch. The 16 memory ports provide an address space in shared memory of 32 Mbytes. Any processor can access any of the 16 memory ports for memory accesses. The entire set of processors may communicate via an interprocessor bus that allows interprocessor interrupts at one of four priority levels, continuously broadcasts a 60-bit nonrepeating clock value, and allows any processor to HALT, START, or CONTINUE any other processor (Ref. 8).

2. **Cm*, a modular multimicroprocessor.** Cm* is a modular multiprocessor system based on the LSI-11 processor. Each computer module is connected via an interface to an intelligent cluster controller. The clusters of computer modules can be interconnected via intercluster buses. Each computer module can share memory with any other computer module in the network through routing tables in the cluster controller (Ref. 8).

3. **C.vmp, a voted multiprocessor.** C.vmp may best be described as a multiprocessor system capable of fault-tolerant operation. It consists of three separate LSI-11 microcomputers, each with its own memory and peripherals. They may run independently as three separate computers communicating through parallel line units, or they may be switched into what is termed voting mode under manual or program control to form a triplicated LSI-11. This form of triple-modular redundancy allows the voted multiprocessor to continue operating under the situation where any one out of three copies of any triplicated element suffers a hard failure (Ref. 8).

III. State-of-the-Art Technology Assessment

In this section an assessment will be made of the applicability of the current spacecraft and fault-tolerant computer technology to an ASM-enhanced spacecraft. In general, design features will need to be added to the spacecraft to accomplish the new functions dictated by ASM. The procurement/management policies are considered adequate for ASM, but new design tools, reliability techniques, and test/validation procedures will be required.

A. Spacecraft Technology Assessment

As indicated in the introduction, ASM consists of spacecraft designs that tolerate failures and that require no ground contact interaction for extended periods of time. The following assessment of current technology is given against these attributes.

1. **Design features.** In each of the presentations there were several methods of fault detection, isolation, and recovery that

were common to all the spacecraft. The methods utilized in the design and implementation have evolved in parallel with the spacecraft requirements. As requirements for long life and high reliability have become more stringent, specialized functions have evolved, with satisfactory in-flight experience serving as the basis for broad acceptance. Typical of the specialized techniques employed by spacecraft to protect against specific fault classes are: cross-strapping, voters, watchdog timers, parity checks, data coding, counters, and switching networks. These fault-handling techniques pertain generally to subsystems. At the system level, about all that is currently done in a fault situation is to put the spacecraft in a safe-hold mode to await ground-operator command. It is the inclusion of onboard detection, isolation, and recovery mechanisms for the purpose of reducing all ground interaction that is the distinguishing characteristic of ASM.

a. *Detection mechanisms.* Present spacecraft design techniques rely on parametric data telemetered to ground operators for fault detection. Generally, faults are inferred from the nonreal-time analysis of such data. However, ASM requires the timely detection of faults by either direct parametric measurement or incipient fault prediction using direct measurement and onboard trend analysis techniques. Because of mass and power constraints, measurement technology becomes a leading technology driver. More extensive use of watchdog timers, parity checks, error-coding schemes, and counters is anticipated. Concerns about the integrity of detection mechanisms, utilizing special test routines and/or additional detection mechanisms must also be resolved.

b. *Isolation mechanisms.* Extremely high reliability switching techniques dominate fault isolation strategies, which involve the ability to remove faulty components from the system prior to reestablishing a "fault-free", fully operational configuration. At issue is the reliability of the switching mechanisms themselves. Redundant switching strategies, power control, and special test routines to assess switch integrity during latent intervals are required.

c. *Recovery mechanisms.* Recovery mechanisms tend to center upon issues of resource management and techniques to maximize system performance subsequent to faults. As such, they represent a system attribute, whereas detection and isolation mechanisms are characterized as subsystem attributes. A system-level view of the available spacecraft resources will be needed, and so system trade-off studies striving to minimize cost (mass, volume, power) and maximize recovery potential from faults are required.

2. **Spacecraft methodologies.** In general, the procurement management policies have been considered adequate by the study participants, however, new design procedures are anticipated.

pated. The following discussion focuses on the need for new design tools and new test and validation procedures.

a. Design tools. Simulators and emulators will be required to provide relative assessments of the design and to assist in trade-off evaluations. Present reliability methods, however, as defined by MIL-HDBK-217 may not be directly applicable to ASM. Areas requiring further study include:

- (1) Software and firmware reliability. The problem increases with the complexity of the software, and total project orientation is needed for success.
- (2) Predictive methodology for transient failure analysis. Test data on commercial computer systems presented during this study indicate that as many as 50% to 90% of reported failures result from transient faults.

b. Testing. The present testing techniques have been shown to be adequate for current spacecraft. For an ASM spacecraft, however, new testing methods may be required because (1) testing of ASM functions must be done at each step in the integration process; (2) new onboard capabilities may require new test equipment; and (3) the possibility of ASM masking a failure prior to launch must be detected.

c. Validation. A major element of validation, specifically relevant to ASM, is reliability validation. As noted at a NASA conference on validation methods research for fault-tolerant avionics and control systems (Ref. 9):

"A traditional approach to reliability validation is the lifetesting method in which one takes n statistically identical copies of the system under test and terminates the test after r ($1 \leq r \leq n$) systems have failed. Using the accumulated time on test, one can derive a point estimate and confidence intervals for the mean life of the system. These statistical techniques also allow one to calculate confidence intervals for system reliability for any given mission time."

"... the number of systems required to be put under test increases monotonically with the reliability of the system being tested. Furthermore, the validation problem is compounded because the cost of an individual copy of the system also increases remarkably with its reliability."

"... applying traditional lifetesting techniques implies unreasonably high validation costs."

The conclusion of the NASA workshop is that a new validation methodology is required for fault-tolerant avionics and

control systems. This conclusion is also appropriate for long-lived, highly reliable spacecraft systems.

B. Fault-Tolerant Computing Technology Assessment

The following conclusions summarize the state of the art in fault-tolerant onboard computers, and the applicability of extending the methodology of fault-tolerant computing to ASM.

1. Machine availability. No fault-tolerant computers are currently available for use on ASM spacecraft. The Air Force's Fault-Tolerant Spaceborne Computer is the most viable candidate for use in a 1985 ASM demonstration, since it is the only fault-tolerant onboard processor in an advanced state of development. A breadboard has been constructed and verified. The major obstacle to its use is the development of low-power, radiation-hardened LSI. This is an enabling technology for all advanced digital systems in USAF spacecraft and is being treated as a problem of high priority and urgency.

The Fault-Tolerant Spaceborne Computer may be hampered, however, because it is implemented as a single uni-processor. It is expected that future spacecraft architectures will tend toward a proliferation of small microcomputers in a variety of control and payload subsystems. Fault tolerance will need to be distributed throughout these distributed architectures (e.g., special fault-detection hardware will be required in each small subsystem computer), and a hierarchy of recovery mechanisms will be employed. Therefore it is important that fault-tolerant distributed computing systems be developed for future generations of ASM spacecraft. The Building Block Fault-Tolerant Computer is a distributed computing system being developed toward that objective. It is not as far advanced in development as is the Fault-Tolerant Spaceborne Computer, but it may be available as an alternative flight system in the future.

2. Fault-tolerance methodology. Many of the techniques employed in fault-tolerant computer design can be extended beyond the computing subsystems to the ASM spacecraft system. This has already been demonstrated to a considerable extent ten years ago in an ASM study of the NASA Thermo-electric Outer Planets Spacecraft (Ref. 10). Some of the fault-tolerant computing methodologies that can be applied to spacecraft are listed below:

- (1) *Careful definition of fault set:* In both digital and spacecraft systems, it is necessary to carefully define and analyze the fault conditions.
- (2) *Fault-detection algorithms:* Following a careful analysis of faults, it is necessary to determine the mechanisms by which they are detected. In both digital and

nondigital subsystems, this takes the form of special sensing hardware and software.

- (3) *Fault containment*: To simplify fault recovery, in both computers and spacecraft, it is necessary to design the system so that the spread of damage caused by a fault is minimized. Whenever possible, it is advantageous to detect and contain faults at the lowest possible level.
- (4) *Hierarchic fault recovery*: Fault detection and recovery in computers is done in a hierarchic fashion. Recovery may be implemented at various system levels depending upon the origin and severity of the fault. This methodology clearly applies to spacecraft systems as well.
- (5) *Reliability modeling*: Reliability and performance models developed for fault-tolerant computers are applicable to ASM spacecraft. The concept of "coverage", which describes the effectiveness of the fault recovery mechanisms, is very important in both computer and spacecraft systems. Extensions of existing reliability and performance models for computers are recommended for spacecraft evaluation.
- (6) *Validation*: Current work on the validation of fault-tolerant computers will be applicable to spacecraft systems. Fault-tolerant computers and ASM design should make it much easier to verify the integrity of the fault recovery mechanisms without inserting faults into the system. Techniques for and results of experimental testing of fault-tolerant computers will be of considerable value to ASM spacecraft engineers.

- (7) *Resource management*: In complex computing systems and in spacecraft there is a resource management problem associated with fault recovery. As an attrition of resources occurs due to faults, the system must optimally allocate those resources remaining.

IV. Summary Observations

Reduction of space system vulnerability can be achieved by moving the control/operations center functions on board the spacecraft. To do this, an autonomous spacecraft maintenance capability is required that (1) incorporates design features that permit the spacecraft to tolerate faults and (2) eliminates the need for routine ground contact. The military spacecraft are currently designed for ground-controlled maintenance, and in terms of the ASM capabilities described above, they cannot now autonomously maintain their own health and welfare. The planetary spacecraft described are a step closer to the goal, but are not there themselves. Thus, although some pioneering work in ASM has been done, it is still in its infancy. In addition to the enhancement of the current capabilities that have already been mentioned, the study group foresees two major technological developments that are needed to enable ASM. These are (1) a fault-tolerant data processing system and (2) an autonomous navigation capability (to reduce the dependence on the control/operations center). The study group is unanimous in its assessment that, with these developments, the ASM capability can be made available.

The ASM-Enhanced System

I. Candidate Design Requirements

Concurrent with the state-of-the-art spacecraft system and fault-tolerant computer assessments, the study group determined a set of ASM system requirements to convey ASM attributes, so that a spacecraft concept could be established. The impact of these requirements on future Air Force spacecraft systems was then analyzed. Following are the candidate conceptual design requirements developed from this study.

- (1) *All Air Force spacecraft launched after March 1989 shall meet the ASM requirements listed below. On this date, the Department of Defense would require all subsequent spacecraft purchased to include the fully operational ASM capability.*

(Prior to this date, it is desirable to add incremental ASM capabilities, consistent with system performance, as they are developed.)

- (2) *The ASM spacecraft shall operate without a ground support control link for up to 60 days without degradation of performance. This is the essence of autonomous operations. The spacecraft will function until ground support is available or desirable from the viewpoint of the ground support team.*

- (3) *The ASM spacecraft shall operate with not more than 10% degradation of key functions over a 6-month period of autonomy. This requirement will set some sizing constraints, such as data storage, and require some definition of loss of performance. It stresses the need for continuous function of the spacecraft on an "ad hoc" basis if scheduled ground support is not provided. The 10% figure is somewhat arbitrary; however, at the end of 6 months, the performance of the entire system shall be at a useful level.*

- (4) *The ASM spacecraft shall interact with the ground support segment for not more than 90 minutes to perform all required support functions without performance degradation. After a period of autonomy, it is required that the spacecraft and ground support perform all the required support functions in this window. The functions include (a) downlink of all stored maintenance history, (b) uplink of all data load (such as star tables and ephemeris), (c) redundancy management, and (d) testing. Specification of the duration of the support window is mission dependent. The intent would be an uplink support*

period approximately the same as that required for non-ASM spacecraft.

- (5) *ASM shall not change the design lifetime of the spacecraft.* The imposition of the requirement for ASM on a spacecraft development is in addition to mission-imposed requirements, particularly the design lifetime. ASM will impact the design methodologies. Such design issues as depth of redundancy must take into account the rate at which resources are used up with the ASM design so that the total lifetime or mean mission duration shall not be reduced.
- (6) *ASM shall not change the performance of the spacecraft or its payload.* All requirements placed upon the spacecraft development for performance of either spacecraft or payloads shall not be affected by the presence of autonomous spacecraft maintenance. The spacecraft must be designed to provide these performance levels in the absence of frequent ground control interaction. Specific additional spacecraft functions, such as navigation, may be required to meet the autonomy requirement. If so, the performance of these functions (e.g., navigation accuracy) must support non-ASM system performance requirements.
- (7) *The ASM spacecraft shall be able to recover from failures that have been defined a priori, and the probability that any particular failure was defined a priori shall be ≥ 0.98 .* The ASM functions include monitoring the spacecraft performance for faults and problem symptoms, and, in the presence of a fault, identifying, isolating, and implementing the recovery mode at both subsystem and system levels. The a priori analysis shall be sufficiently complete that, during the lifetime of the spacecraft, at least 98% of the failures (e.g., where some component has failed) will be identified in this manner (the coverage is $\geq 98\%$). Compound failures wherein multiple symptoms occur simultaneously or near simultaneously during the detection and recovery period can be exempted from this requirement.
- (8) *Following launch, the ASM spacecraft shall go through a period of on-orbit checkout and initialization of the same duration as that of a comparable non-ASM spacecraft.* The autonomy requirements discussed here are applied to the operational period of the spacecraft, which is deemed to begin following the on-orbit checkout period. In the checkout period, maintenance will be under ground control, with autonomous capabilities turned on or off as appropriate. Since the addition of ASM does add certain

functions, operating modes, and complexities to the spacecraft, these must also be checked out during the same period. Following checkout, all autonomy requirements will apply.

- (9) *The spacecraft shall process and store all onboard management data required for ground support, and shall telemeter the data during the ground support periods upon ground command. The capability shall handle all necessary data for 6 months.* No matter how confident designers may be of the maintenance capability of the spacecraft, it will be necessary to leave a record for ground support (an audit trail). Without this information, the ground support function cannot evaluate the state of the spacecraft and use the record of performance to extend the lifetime of the spacecraft, develop or implement alternative operating modes, or improve future designs.
- (10) *The ASM spacecraft shall transmit a message to the ground at the first opportunity following any onboard fault-management activity.* Whenever an incident occurs that requires maintenance activity in response to failure symptoms, it is important that the ground be given the opportunity to review the action and to verify the status and mode of the spacecraft. Thus, a telemetry message indicating that some activity had taken place would be sent to the ground at the first pass over an appropriate ground station. This type of signal may be coded into the user data to trigger an alarm at the ground support station. Sending of the message does not abolish the obligation of the spacecraft to retain the data for the maximum period, and to continue to operate in an autonomous manner for the established periods.
- (11) *The ground support shall be able to override ASM management activities for the system and the subsystems.* While the ASM spacecraft shall have the ability to perform redundancy management in the presence of an apparent fault or problem, it is necessary that the ultimate control over these functions be maintained at the ground, and that the spacecraft shall allow for ground communication that overrides and can reverse the prior decisions of the ASM functions. The capability is necessary so that the system will be able to recover from such learning curve uncertainties as misdiagnosed problems or design flaws. In this way, nonfailed components may be recycled back into the configuration inventory, or the spacecraft alternate modes of functioning may be utilized to make use of partial capabilities of components. In terms of a hierarchical decision tree, the ground support personnel shall occupy the top level to maximize system performance.

- (12) *The source of last resort for fault isolation and recovery shall be the ground support.* The ASM spacecraft shall be designed to recognize when it has been unable to isolate, remove, and recover performance following a fault. When this occurs, the spacecraft shall take action to protect itself from self-injury or dissipation of resources (such as an engine firing limit cycle that would consume propellant), and await ground intervention.

Satisfying these design requirements implies the movement of the control of routine maintenance operations from the ground to the spacecraft. The ground segment will assume a supervisory role, always maintaining the ability to override ASM actions, but allowing the spacecraft to initially handle its own maintenance functions. The space segment, on the other hand, will become more complex due to the added operations it must perform, including onboard navigation (eliminating the need for routine uplink) and fault detection, isolation, and recovery. To handle these added operations, a fault-tolerant data processing subsystem and an autonomous navigation subsystem will be required. The major benefits of ASM would then include: (1) reduced system vulnerability, because it is no longer dependent upon the ground station or possible incorrect commands by human operators, and (2) faster recovery from failures (seconds instead of hours or possibly days) because recovery procedures would start immediately upon fault detection.

II. Impact on the Ground and Space Segments

Some examples of operations and maintenance functions that presently are accomplished by the ground segment, but with ASM will be accomplished by the spacecraft, include:

- (1) Attitude/pointing commands
- (2) Thermal control loop
- (3) Power management
- (4) Fault monitor/isolation
- (5) Fault tolerant computation
- (6) Fault switching
- (7) Load switching
- (8) Trend analysis

A reduction in ground control activity can clearly be seen. It should be remembered, however, that in its supervisory

capacity, the ground segment will have the ultimate authority and responsibility in all situations. As total reduction in ground control will not occur at one time, a transition phase will be required. This phase will enable: (1) inflight measurements of effectiveness for ASM over a diverse set of operating conditions, (2) the development of understandable and predictable ASM operations, and (3) simultaneous support of both ASM and non-ASM operational spacecraft.

The increase in spacecraft autonomy will mean an increase in the complexity of the spacecraft. While this increase in complexity must not introduce catastrophic failures or reduce the payload performance, it will tend to increase the spacecraft's mass, power consumption, and total cost. Given the study group's knowledge of current and projected technology, the following heuristic estimates were established as reasonable design goals for an ASM-enhanced spacecraft:

Power consumption:	ASM < 10% of total
Mass impact:	ASM < 5% of total
Cost impact:	ASM < 10% of life-cycle cost

III. A Hierarchical Description of the Space Segment

The following sections describe what the study participants believe will be the impact of ASM on a generalized spacecraft system. In these descriptions, the following assumptions have been made:

- (1) The ASM requirement is added to a new spacecraft before design.
- (2) ASM technologies will be available.
- (3) Payload is treated as a subsystem, except for user data flow.
- (4) As long as mission objectives are met, normal spacecraft functions may be interrupted during certain fault recovery procedures.

A. System Architecture

System architecture evolves from the mission requirements, and includes the hardware organization, data flow characteristics, and (if a digital system) the hierarchical operating system. The system must judiciously allocate the available resources and, upon command, must report all ASM actions (including parametric data) to the control/operations center. Finally, it must also insure its own integrity (through self-diagnosis) so that incorrect actions and ground system lock-out modes are eliminated.

An example of a system architecture that could be used for ASM is shown in Fig. 3. This is characterized by both distributed and central processing system attributes. Efficient management of the spacecraft resources based upon prespecified algorithms require centralization of high-level decision making. This would be accomplished by a fault-tolerant processor, serving as the spacecraft central controller, augmented by processors located in each of the subsystems as appropriate. In addition to the new subsystems already mentioned, the architecture should also accommodate additional mission-unique subsystems.

The system architecture example described above is one of several possible architectures for an ASM spacecraft. While a detailed investigation of the various architectures was not a part of this study, the participants believe that such an effort

should be undertaken as one of the first tasks of an ASM development program.

Whichever architecture is chosen, the study group believes that a "layered" fault protection scheme should be used, enabling fault containment at the lowest possible level to minimize subsystem interdependencies resulting from fault propagation (including data contamination). This fault protection scheme is illustrated in Fig. 4. In this scheme, individual subsystems, under system control, will diagnose local failures and take corrective action. Ambiguous problems resulting from failures within the interfaces between subsystems will require diagnostic routines and hardware to pin-point the failure. Some unresolved system issues include the problems of transients, false failure alarms, multiple faults, and faults within the fault-tolerant computing system. Once the system has been designed, test and validation procedures must be

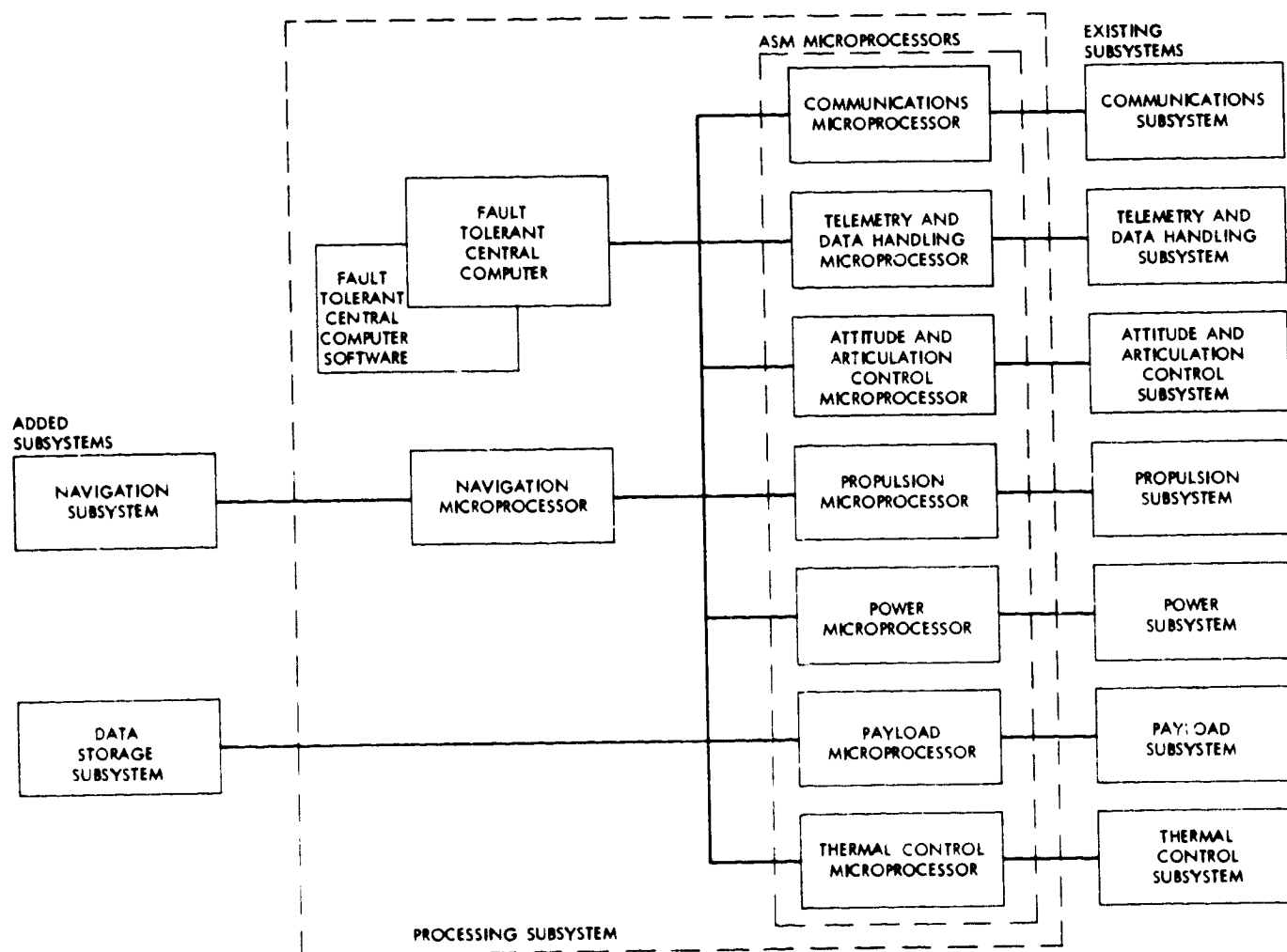


Fig. 3. Example of a system architecture for ASM spacecraft

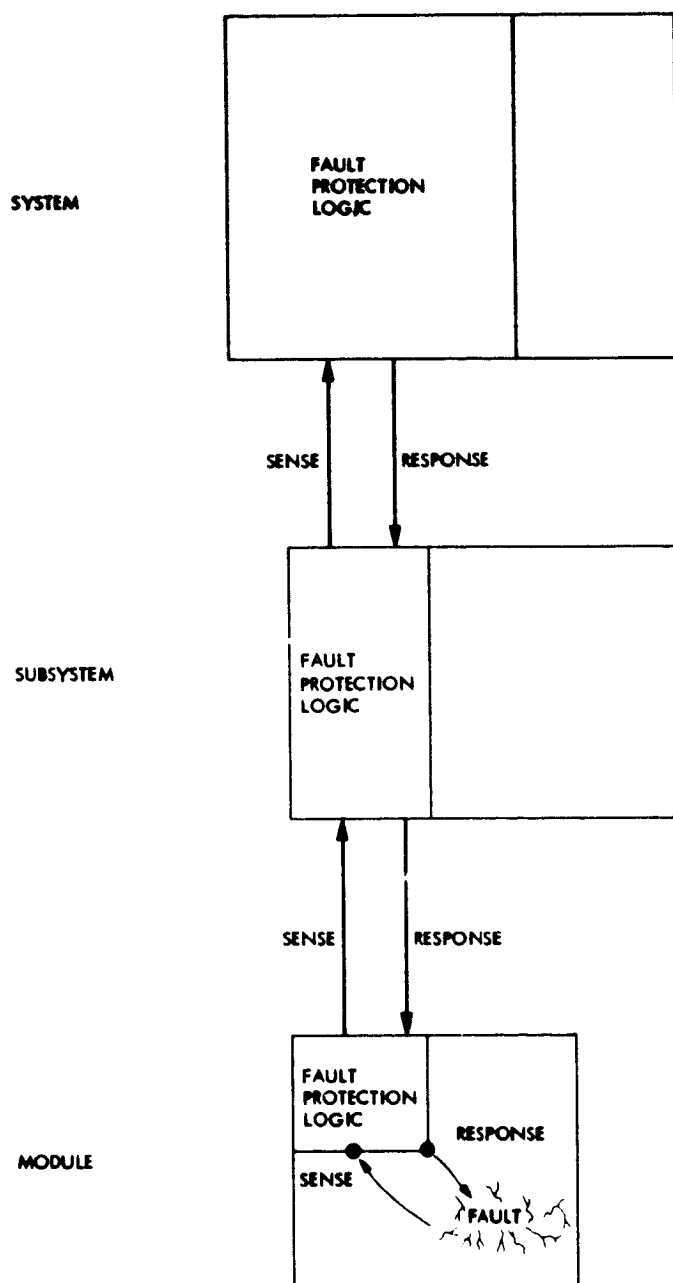


Fig. 4. "Layered" architecture of fault processing

formulated. Finally, there should be a demonstration program showing that the requirements for ASM are met without compromising either the mission lifetime or payload performance.

B. Subsystem Impact

ASM will affect the traditional subsystems (attitude and articulation control, power, telemetry and data handling, payload, communications, propulsion, and thermal control) by requiring that they add the capability of diagnosing and handling their own faults. The conceptual design requirements imposed on the ASM spacecraft, however, necessitate the potential addition of two new subsystems. These include a fault-tolerant data processing subsystem and an autonomous navigation subsystem.

The need to integrate independent subsystems with individual processing requirements into a control hierarchy for the purpose of managing and reporting fault-protection leads to a requirement for a fault-tolerant data processing subsystem. Because of the potential for power-interrupt failure modes, this subsystem must include limited nonvolatile backup memory resources for selected critical program and data storage.

The requirement for six months of unattended operations necessitates an autonomous navigation capability. The problems of vehicle position and velocity are dependent upon mission requirements for attitude control and pointing. It involves the characterization (modeling) of complex gravitational fields, including the effects of Earth figure and multibody (Earth, Moon, Sun) interactions that perturb the vehicle position and velocity. As attitude control requirements become more stringent, more precise models and advanced sensors permitting real-time drag acceleration measurements will be required to complement existing inertial measurement devices and celestial sensors.

Finally, the requirements for a six-month audit trail and onboard trend analysis to permit fault prediction and protection necessitates storage and manipulation of a large volume of data. Without ground links, the study participants believe additional data storage capabilities, coupled through the data network to the other spacecraft subsystems, will be needed.

Implementation Plan

I. Introduction

This section, together with the Research Agenda of the next section, describes the study participants' recommended plan of attack to solve the problem that prompted the ASM study: to satisfy the requirement for spacecraft readiness in the face of the loss of ground stations. In contrast with the Research Agenda that addresses medium- and long-range academic research for an advanced ASM system of the 1990s, this section focuses on the near-term (next five years) industrial technology development and, most importantly, the earliest possible system-level, proof-of-concept demonstration. The plan stresses delivery of "product" in a steady stream from subsystems to a complete system for the System Program Offices' consideration and introduction into flight programs. In this sense, the plan is a technology program that is managed like a project, with focused goals and milestones to be met. While there is no provision for a flight demonstration in this plan, a definite goal has been to provide a program that will generate continuous ASM technology "fall-out," which can be utilized in ongoing programs and in design block changes.

The program described below is preliminary; the limited resources of the study precluded a detailed program development and cost estimate. However, the study participants feel the proposed plan described contains the essentials of a workable program needed to meet the future requirements of the Air Force.

A. Purpose

The purpose of the plan is to recommend a coordinated set of developments that will give industry a demonstrated capability to build an ASM spacecraft, and hence, enable the Air Force to change from ground-dependent to autonomous operational spacecraft by 1989.

B. Goals

The goals of the plan are:

- (1) To develop an ASM technology and apply it as early as possible to existing programs, especially DMSP, DSP, GPS, and DSCS III.
- (2) To develop, by 1985, a demonstrated industrial capability to produce autonomous spacecraft, so that the first operational launch may take place by 1989.

C. Approach

The approach taken in preparing the plan can be summarized in the following points:

- (1) Involve as many relevant governmental and industrial organizations as possible. This will create a broad base of ASM experience, design, and methods.
- (2) In support of the first goal, begin work with existing subsystem designs; ASM implications and problems

must be characterized, designs and breadboards must be modified, and results demonstrated early.

- (3) In support of the second goal, begin work on a parallel system-level analysis, design, and hardware program leading to a proof-of-concept demonstration.
- (4) Use as much available hardware as possible. Develop and build as little new equipment as possible to meet requirements. Acquire engineering test models of actual and/or representative systems/subsystems of Air Force satellites.
- (5) Focus on ASM-required changes only; design life and performance advancements not needed for ASM should not be pursued.
- (6) Hold frequent reviews and conferences for technical information exchange with all concerned industrial, academic, and government organizations.

II. General Plan Description

The study participants recommend that the program consist of four major elements, prefaced by a three-month start-up period: first, an activity addressing existing programs at the subsystem level, producing demonstration products within two years; second, a system-level project addressing ASM-enhanced Air Force programs with proof-of-concept in five years; third, applications research directed at filling technological gaps; and fourth, an advanced system development, aimed at the 1990s, to provide an opportunity for unconstrained research to expand capabilities beyond the foreseeable future. These elements are denoted as Tasks 1, 2, 3, and 4 respectively. The advanced systems development, Task 4, is identified for completeness, but because its products would not meet the 1989 launch requirement, resources are not identified. The Research Agenda elaborates Task 4.

A general view of the plan is shown in Fig. 1, in which the arrows indicate typical points of technology transfer between tasks to the System Program Offices. All tasks start at the beginning of CY81 to allow program definition and start-up to take place in the first three months of FY81. Task 1 is a two-year activity that assesses increased fault detection, isolation, and recovery for existing subsystems. Design changes will be made and breadboard units will be modified to test ASM capabilities and benefits. Task 2 is a 5-year activity that includes a top-down system development and the necessary new subsystem technology developments required for ASM. A pre-Phase A effort is required to prepare a procurement specification and to select the contractor for both Task 2 and Task 3. In Phase A, the mission requirements and spacecraft design will be established, while in Phase B, the fabrication,

integration, test, and demonstration of the ASM system will be performed. Task 3 is a five-year applications effort required to develop new well-defined subsystem technologies. Task 4, through CY85, is performing the basic research for a "second-generation" ASM system as mentioned earlier.

III. Task Descriptions

The layout of the entire program is shown in more detail in Fig. 5. In the view of the study participants, the plan represents the best method of addressing the urgency of obtaining an ASM readiness, given the available resources. The relative times needed to accomplish the objectives are shown; reduced funding or delays in program start-up will result in commensurate delays in completing the tasks described below.

A. Task 1: Existing Subsystem Redesign to ASM

The first task is a 24-month effort to characterize the subsystems involved with ASM, redesign the breadboards, check-out subsystem ASM functions, and provide measures of capability required to accommodate ASM. These measures will be in such terms as memory size and throughput. Because the subsystems are well known, it is felt that modifying them to include ASM features will be the quickest and most cost-effective way to size the challenge early and to incorporate some ASM capability into the spacecraft. When successfully demonstrated, the System Program Offices could consider them for operational use.

It is expected that much of the design work, and perhaps the breadboards, would be important to the Task 2 effort, and heavy interaction between tasks should be anticipated. The subsystems to be studied are (ranked by their ASM importance): attitude and articulation control, power, telemetry and data handling (including tape recorders), payload, communications, propulsion, and thermal control. Structure and mechanical devices are not included because their design is little impacted by ASM requirements. It is recommended that two contractors perform on each subsystem to gain a diversity of experience for contractor and program application. As no two designs are the same, additional information will be gained from this approach to broaden the data base.

The first six months is spent on design study. The subsystem's fault characteristics will be examined, and the fault detection, isolation, and recovery techniques will be developed. The hierarchical assignment of fault recovery between faults totally handled within the subsystem and those "passed on" to the system for action, will be developed. Evaluation of the reliability of sensors and switching, which are essential to "error free" ASM, will be done. Changes in design techniques, instrumentation, and associated software or firmware as well

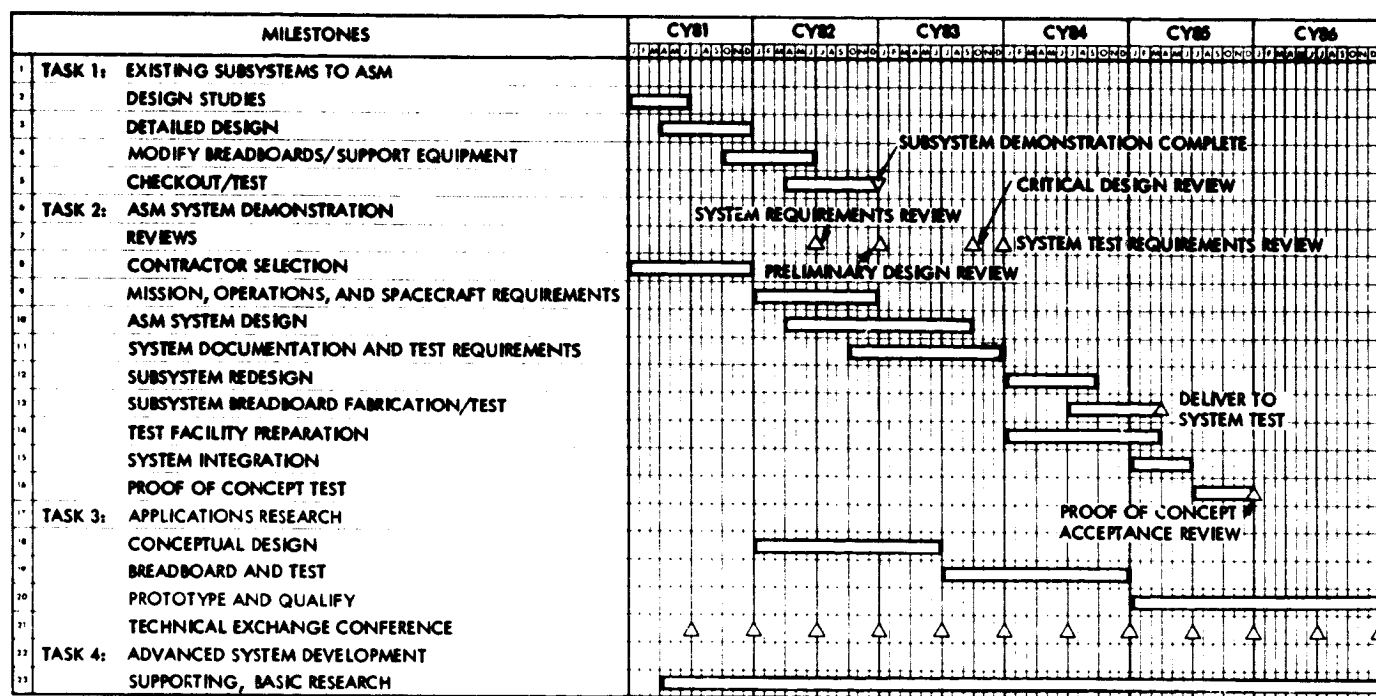


Fig. 5. Autonomous spacecraft maintenance program

as the hardware will be covered. An assessment will be made as to what benefits accrue in reduced ground maintenance with the recommended ASM capabilities in the subsystems. In the next nine-month period, detailed design takes place. Algorithms for ASM will be defined, coded, and debugged. Hardware modifications and software changes will be made. ASM design features may be implemented in single-string fashion so that in this exercise only the subsystem under test will be fault tolerant.

In the last year of the program, the breadboards or engineering test models and associated support equipment will be modified to include the ASM features, and then tested. The testing will be a rigorous exercising of the fault-processing logic by injection of all types of faults. The testing will provide specific valid measures of ASM performance and design requirements in such terms as memory requirements, speed, and recovery algorithms, which can be utilized by various program offices as appropriate in their ongoing or new programs.

At the conclusion of Task 1, impacts of ASM will be clearly established. Fault character will be understood, new sensor and switching technology will emerge; software and hardware will be sized to do the job; algorithms for handling faults will be checked out, many system issues will be discovered for resolution in Task 2, and finally, the System Program Offices will have an opportunity to assess ASM applicability at the subsystem level.

B. Task 2: ASM System Demonstration

This second recommended task is a five-year activity that ends in a system-level demonstration of ASM. It is laid out very much as a typical flight project might be, but truncated at the system test of a prototype spacecraft with no flight hardware built. The assumption is made that the system demonstration will be achieved by applying ASM to one mission, such as DSP, DMSP, or GPS, but the extension of this ASM technology to all Air Force missions will be an active design consideration. The reviews are typical, with only the System Test Requirements and the Proof-of-Concept Acceptance Reviews being unique to this program. The phases are typical as well: systems analysis and requirements generation; system design; subsystem design, fabrication, and test; and system integration and test.

The analysis and requirements activity proceeds during the second year and culminates at the Preliminary Design Review with the production of the Mission and System Requirements document. The activity includes mission impacts, recovery strategy, degradation profiles, and data return strategy as faults occur; reliability and risk analyses; operation analysis with ASM; flight/ground tradeoffs; spacecraft system fault analysis; development of the "layered" fault protection system architecture, fault detection, isolation, and recovery at the system level; payload interaction with ASM; and in-flight navigation requirements generation.

The ASM system design occurs during the second and third year, culminating at the Critical Design Review. The design team will study alternate design approaches; allocate functions between hardware, firmware, and software; study distributed vs central computing; analyze performance; write specifications; and have the usual heavy system/subsystem interaction on design (including Task 1 personnel). The key product will be the Spacecraft System Specification, available at the Critical Design Review. Another important part of this period is the system test requirements to be imposed. The design must allow access for fault injections during test, which may not be easy to implement. The System Test Requirements Review will address adequacy of testing to prove that ASM has a flight-ready capability.

The fourth and fifth years of the ASM system activity will be used to redesign, fabricate, and test the subsystems, and then integrate them and test the system for proof of concept. Where possible, the subsystems from Task 1 will be used, but modifications will still have to be made to integrate them into the overall system design. Redesign, fabrication, and test should take 15 months. The subsystems will be delivered to system test at 51 months into the project.

The test facility preparation starts at the beginning of the fourth year, and must be completed by subsystem delivery. Support equipment must be designed or modified as needed. It must be determined how the fault injection and testing will be done for proof-of-concept testing. In addition to the different states that the facility will have to test, it must also be able to simulate the power source, thrusters, spacecraft dynamics, and mechanical devices.

Finally, system integration begins at 48 months, and proof-of-concept testing begins at 54 months. The system-level proof of concept will be a full electrical demonstration of the ASM system, under the test conditions already mentioned. Testing will be performed in a laboratory ambient environment.

Throughout the program, attention will be paid to any spacecraft block changes to ongoing programs that may provide an early opportunity for ASM application. Block changes will not necessarily affect the ASM system demonstration project, but if one occurs at an opportune time, some of the system development may be directed toward it.

The Proof-of-Concept Acceptance Review is the final milestone in the system activity. Test results would be examined for validity and completeness, and if the review is success-

ful, ASM will be demonstrated as a viable, implementable technology.

C. Task 3: Applications Research

Task 3 is a new technology research and development activity of five years duration that addresses known gaps at the subsystem level. Two are currently identified: a distributed fault-tolerant data processor with a nonvolatile computer backup memory, and an autonomous navigation subsystem. Figure 5 shows the development schedule for these items. It is expected that the breadboards for these subsystems would be used in the system proof of concept. If not available, appropriate simulators/emulators would have to be provided. Resources for in-flight navigation are not included here because it is assumed that currently-funded programs elsewhere can be expected to produce the needed breadboard in 1983.

D. Task 4: Advanced ASM System Development

As mentioned earlier, this effort is comprised of the Research Agenda of the next section. The products of that research will fold into the "second-generation" ASM system of the 1990s.

E. Program Cost Estimate

A budgetary cost estimate for Tasks 1, 2, and 3 is shown in Table 7. This does not include funds for the development of the autonomous navigation capability, which is assumed to be handled in another program. These figures should be considered only an estimate for several reasons. First, the cost of developing the new technology is not well known. Second, a specific mission application has not been assumed, and so candidate spacecraft could not be assumed. Finally, substantiating data was not provided by the individual participants. For these reasons, a more definitive cost study should be performed in the initial phases of the activity.

IV. Summary

The Implementation Plan presented here, in the view of the study participants, represents a balanced, focused attack on the Air Force's spacecraft maintenance problems. System, subsystem, and new technology elements are all pursued at a level sized to the difficulty of the specific ASM challenge while recognizing the needs for early demonstrable results for ongoing operational programs. The above described implementation plan is recommended by study participants as the basis for the Air Force's ASM program.

Table 7. ASM program resource estimate

Task	Program element	Program resources, \$k ^a					Totals
		CY81	CY82	CY83	CY84	CY85	
1	Existing subsystems ^b redesign to ASM	2,900	3,500	800			7,200
2	ASM system design ^c and demonstration	500	4,500	7,500	7,500	3,000	23,000
3	Applications research	600	800	1,300	2,300	1,200	6,200
	Totals	4,000	8,800	9,600	9,800	4,200	36,400

^aContractor costs only. AF procurement and management costs not included; autonomous navigation development not included.
Figures are FY80 dollars.

^bTwo contractors per subsystem assumed.

^cSingle-system contractor assumed

Research Agenda

I. Introduction

A research program to support the development of automated spacecraft maintenance must focus on the most critical problems expected in that development. A major challenge is to channel a great deal of fault-tolerance expertise, developed for other applications, into work that will specifically benefit the space program. Fortunately, most of the ASM spacecraft problems are shared by many other applications (e.g., process control, avionics, and robotics) and are sufficiently general in scope to be of considerable interest to the academic community. This proposed Research Agenda is organized around specific spacecraft development problems. An underlying cause of most of these problems is increasing complexity. The basic motive force is rapidly expanding capabilities of LSI and VLSI technology. Until very recently, satellites contained a few hundred to a few thousand integrated circuits. Each integrated circuit contained a few gates or registers, and the collection of integrated circuits were combined to form a system. We will soon fly single VLSI chips that contain thousands of gates and memory cells such that each chip is itself a complex subsystem in a tiny package. This can result in an enormous increase in functional capabilities in satellites. Onboard navigation, very-high-performance signal processing, threat evasion, pattern recognition, and a host of other capabilities will become feasible.

It is expected that fault tolerance will be an important attribute of VLSI design because of the problems of transient faults and testability. The very high complexity of large VLSI systems is expected to result in transient faults every few minutes, or every few hours. Current experience indicates a transient error rate in LSI memory of one error per hour per million bits. Even if this rate is reduced an order of magnitude, impaired operation will occur unless the spacecraft system is designed to detect and recover automatically from these fault conditions. The problem of thoroughly testing complex VLSI circuits has only recently been recognized. Many existing devices are essentially untestable and design faults are uncovered in the field after prolonged usage. Since the only access to a finished device is through a limited number of pins, it becomes nearly impossible to exercise all internal states of a device containing thousands of transistors. Testable design methodologies have been recognized as a high-priority research problem in industry, and is even more critical for space applications.

New and largely unexplored problems are expected at the system architecture level of space systems. Proliferation of specialized microelectronic controllers in spacecraft subsystems will lead to more complex cooperation between subsystems, between the spacecraft and ground, and perhaps between different spacecraft. Consequently, the system organization, software, and fault-tolerant aspects of space-

craft will have to become correspondingly more complex. A hierarchy of computing processes is envisioned. This implies more onboard monitoring circuitry to detect faults before errors propagate through the system, making diagnosis and recovery extremely difficult. Automatic trend analysis may be employed to record and discover new error patterns, and heuristic recovery algorithms may be required to recover from unanticipated faults.

In summary, there exist a variety of research areas that are rich in both substance and applicability, and are essential to the development of future space systems.

II. Research Plan

Recognizing that resources are limited, the following research plan is broken into five areas that are essential to future ASM development: (1) VLSI technology, (2) architecture of advanced ASM systems, (3) software fault tolerance, (4) modeling and analysis, and (5) supporting development. In terms of criticality, they are listed in descending order. Subsystem technology and especially related VLSI issues must be resolved no matter what architecture is chosen. An understanding of system architecture is necessary to make modeling and analysis more useful and relevant.

A. VLSI Technology

Testing of LSI devices is a serious and expensive problem in current spacecraft. It will be a critical issue in ASM systems because it is necessary to detect faults very quickly after their occurrence, so that autonomous recovery mechanisms can restore the spacecraft to normal operation with minimal disruption of performance. This research area has two components: (1) self-testing VLSI, and (2) on-chip redundancy.

1. Self-testing VLSI. The first goal of this component is to develop methodologies to design VLSI chips that are (1) thoroughly testable prior to normal operation, and (2) self-checking. A methodology for designing self-checking circuitry has been developed that allows the chip to detect internal faults concurrent with normal operation. We must learn to design a chip that will be fully exercised and tested during normal operation. Even if we can detect a fault when it occurs, it may be months or years before a complex chip in normal operation enters a faulty state. Thus, development of "easily" testable circuits is a high-priority research item.

2. On-chip redundancy. A second goal of this research is to investigate the use of on-chip redundancy to improve yield and chip reliability. Although the existence of catastrophic failure modes make it necessary to back up individual chips with

spares, the use of on-chip redundancy may greatly improve chip reliability and system life.

B. Architecture of Advanced ASM Systems

This area includes the hardware and software organization to achieve fault tolerance in highly complex ASM spacecraft. This work must take into account the trend toward proliferation of computers in spacecraft subsystems, and it should be directed toward future space systems in which dozens of distributed computers may be used. It should address the impacts of VLSI in spacecraft architecture, performance, and ASM capability. It is expected to support ASM spacecraft development beyond 1990.

To effectively involve the academic community in spacecraft system research, it will probably be necessary for the USAF to develop a set of strawman system requirements. Most members of the academic community are not familiar with the unique problems of space systems (e.g., power, weight, volume, uplink and downlink, instruments, testability, command interfaces, and subsystem operation). Thus careful problem definition is required to focus this work toward real space problems. Such strawman systems might include a robot for in-space assembly, or a satellite that must correlate and make decisions on multiple sensor inputs.

The following architectural tasks are highly interrelated (e.g., hardware and operating systems studies), and mechanisms for frequent interchange of information between groups working in this area are very important. A series of workshops might be one such mechanism.

The following tasks have been identified: (1) organization studies, (2) operating systems for large hierarchic space systems, (3) recovery by problem solving, (4) fault tolerance in very-high-performance processors, (5) architecture development.

Underlying Tasks 1, 2, and 3 is the need to develop a hierarchic model of complex distributed functions in ASM spacecraft, and models of the interfaces between spacecraft subsystems. Computing in each spacecraft subsystem generates a "virtual" digital interface between the subsystem and the spacecraft system. Models of these interfaces should include generalized fault monitoring and recovery functions at each level of the hierarchy. Such models may lead to insights on how to structure these interfaces to improve software reliability, and fault recovery, as well as simplified commanding and system integration.

1. Organization studies. These studies will include postulating fault-tolerant distributed, and hierarchical computer architectures along with communication formats, and software

executive structures that are applicable. The first goal of this component is to perform tradeoffs and pinpoint the relative capabilities and limitations of the postulated architectures with respect to spacecraft performance and fault tolerance. The second goal is to develop specific fault-tolerance techniques for use in these types of systems. Among the fault-tolerance questions to be addressed are:

- (1) How can reliable clocking and synchronization be carried out between the multiple processors?
- (2) How can embedded processors with their numerous input/output pins be spared?
- (3) How can nonhomogeneous specialized processors be handled, especially when fault-tolerant architectures are biased towards a homogeneous pool of processors?
- (4) How is executive software organized to support recovery, rollback, and diagnosis?
- (5) Can the system be designed to tolerate software errors through fault-containment?
- (6) How does one design virtual interfaces that partition software between various computer modules?
- (7) How is redundancy distributed? What fault detection is provided at the various sensor/actuator levels within the computer, subsystem, and system levels? What are the levels of sparing employed on chips, between chips, and between subsystems?
- (8) How well can fault-tolerance features be made transparent to the user?

2. Operating systems for large hierarchic space systems. This research is directed at developing operating system concepts best suited to complex distributed systems. Issues to be addressed are:

- (1) Hierarchical partitioning of executive functions - global/local.
- (2) Effect of alternative executive structures on application software reliability, testability, and fault-containment.
- (3) Interaction of executive with hardware and software fault-tolerance mechanisms.
- (4) Provability of correctness of the executive.
- (5) Robustness - the ability of the operating system to survive errors in applications software.

3. Recovery by problem solving. Many of the techniques of artificial intelligence and problem solving may be applicable in dealing with unanticipated fault conditions, or with operator errors. This task is intended to develop heuristic techniques to

deal with this class of unexpected faults and possibly some errors.

4. Fault-tolerant high-performance processors. This area includes the processors that will be or are being developed (e.g., signal processors). Techniques to achieve fault detection and recovery, and also to integrate such systems in ASM satellites, require investigation. This is especially true because many of these systems will probably not work without embedded fault tolerance due to a high transient error rate brought on by enormous complexity.

5. Architecture development. To use ASM in a satellite, the supporting technology must be in place. Project offices are usually in no position to accept the delay and risk of developing new technology. Thus, this research program should develop one or more fault-tolerant computer system architectures to at least the breadboard stage. Fault-tolerant architectures are sufficiently complex that it is necessary to build and test them to understand their behavior. It is expected that the selection and design of these architectures would be outgrowths of current architecture developments (Software Implemented Fault Tolerance, Fault-Tolerant Multiprocessor, Fault-Tolerant Spaceborne Computer, and Building Block Fault-Tolerant Computer), which would be heavily influenced by the organization studies above.

C. Software Fault Tolerance

This research area is concerned with developing reliable software for distributed computer systems for ASM spacecraft. It includes three areas of study: (1) system partitioning and interface definition to improve software reliability, (2) self-checking flight software, and (3) fault-tolerant software.

1. Partitioning and interface definition. This task is tightly coupled with the architecture studies. The partitioning of functions within a distributed system and the virtual interfaces between subsystems have a very large impact on the complexity and reliability of applications software. The goal of this research is to study tradeoffs between alternate partitioning and interface (command and data) definitions and their impacts on software complexity and reliability. (Such issues as the degree of system vs local control of a subsystem, timing requirements on commands, acceptable communications delays, scheduling strategy, and internal software structure, are involved in these studies.)

2. Self-checking flight software. One goal of this task is to develop methodologies for detecting faults in applications software as it is performing its normal operations. This includes the inclusion of acceptance tests in the flight programs

and a variety of other software fault detection mechanisms. A second goal of this task is to develop verification and validation techniques, to prove the effectiveness of this self-checking code.

3. Fault-Tolerant software. This task is intended to develop techniques for developing software that operates in the presence of programming errors. This is a difficult area that involves the use of software fault detection and the execution of redundant code to recover from design faults.

D. Modeling and Analysis

In the development of advanced ASM spacecraft systems, it is necessary to develop experimental testing techniques to verify the effectiveness of the built-in fault-tolerance mechanisms. Analytic statistical models that use these experimental results and component failure rates are then required to predict the reliability and performability of the ASM spacecraft as a function of time. This type of modeling is essential to determine if a given spacecraft design will meet its objectives, or to perform tradeoffs between competing design approaches.

A second class of tools needed in ASM development are functional models and design languages that can facilitate design and verification of ASM systems. Such tools could provide the capability of specifying and simulating operations of proposed systems, and allow changes and improvements before a design is locked into hardware. A second important use of design languages and functional models is to provide a basis for formal verification of a design before launch, and validation of command sequences to an orbiting ASM spacecraft.

The modeling and analysis area is broken into three components: (1) experimental testing, (2) statistical modeling, and (3) functional description, modeling, and verification.

1. Experimental testing. Spacecraft testing, already a difficult problem, will become considerably more complex with the introduction of ASM. A significant problem is how to test these functions that are dedicated to autonomous maintenance. The goal of this component is to acquire a deeper understanding of testing problems peculiar to ASM, and develop test generation and test applications methods for solving these problems. Among the problems to be considered that complicate testing are: (1) testing at many levels in a hierarchy, (2) the possibility of many combinations of input events and many unanticipated faults, (3) the need to test in an artificial environment, (4) wear-out phenomena, and (5) the development of specific tests required by statistical reliability models.

2. Statistical modeling. Probabilistic models of ASM spacecraft are needed to assess the probabilities of performing at various levels, ranging from full performance to failure, over the projected life of the spacecraft. Such models are being developed, but have yet to be extended to complex, heterogeneous spacecraft systems. The goal of this component is to extend current methods, developed primarily for computer applications, to accommodate additional complexities in large, heterogeneous spacecraft systems. A considerable advancement is required over existing models to deal with the complexity resulting from dependent subsystem failures, and the models must carefully relate to testing results as input parameters. Special emphasis must be placed on modeling and analysis of transient faults, since transients are expected to be a major problem of VLSI technology.

3. Functional description, modeling, and verification. Spacecraft systems are complex, multifunctional real-time systems with many different types of physical subsystems. Although functional models may exist for many subsystems, functional descriptions at the spacecraft level are typically informal and incomplete. With the additional complexities of VLSI and autonomous maintenance, informal design methods, particularly at the system level, may no longer produce the desired results (witness the evolution of computer operating system design methods).

One goal of this component is to investigate whether design languages, such as those being used in the context of computer and computer-based systems, can be usefully extended to facilitate spacecraft design. Of particular relevance are languages that call for timeliness, fault tolerance, distributed resources, and concurrent (parallel) execution of tasks.

A second related goal is to develop uniform functional models (abstract representations) of autonomously maintained spacecraft. The models sought are hierarchical models that relate high-level functional behavior of the total system to lower-level subsystem functions and interactions, both during normal operation and in various modes of fault recovery or of degraded operation. This type of model can facilitate the design process and may, in the future, lead to design automation tools for spacecraft design. Functional models might also be used to formally verify the system.

With the increase in logical complexity required for advanced ASM spacecraft, model-based evaluation and testing may not suffice to provide the desired confidence in the system. The third goal is to investigate the possibility of extending formal verification methods (such as those being developed for programs, operating systems, and at least one avionics processor) so as to apply to formal descriptions of spacecraft.

The areas of specification language, formal functional models, and formal verification techniques are intimately related, and are thus grouped into one component in this plan. This represents long-term, high-risk research, but the payoff can be enormous.

E. Supporting Development

Two supporting developments have been suggested by the research group. The first, of immediate urgency, is ASM data base development. The second is development of a spacecraft laboratory for ASM integration patterned after a similar development within NASA.

1. Data Base Development. A comprehensive data base should be established for ASM development. It should serve as a repository of two types of data.

The first is statistical data required to determine values of parameters for reliability and performance models. Currently used data is often incomplete and inaccurate. Data sought should include piecepart failure data (particularly transient failures), data on VLSI failure mechanisms, and data on sub-

system failures, system failures, and that on the environment gathered from past missions.

The second type of data is information on existing (perhaps generic) spacecraft systems and subsystems, and information on redundancy and ASM techniques already being used on spacecraft. There is a significant problem of technology transfer between spacecraft designers and researchers. This type of data base would provide a multidiscipline exchange that may be indispensable in advancing the state of the art in ASM.

2. Spacecraft Laboratory. This is a much more ambitious development. It would consist of a computing facility for ASM spacecraft integration (analogous to NASA's Airlab for avionics systems). This is envisioned as a facility where spacecraft simulations would be provided. New hardware/software subsystems could be integrated and tested using the system, and new system designs could be developed and simulated. Such a facility would be used for experimental testing of prototype spacecraft systems. It would be national in scope and provide both access and a focus for information exchange between manufacturers and researchers.

Conclusions and Recommendation

ASM is a logical, evolutionary change to the Air Force's concept of space system operations that results in the transfer of functions from the ground segment to the space segment. With ASM, the role of the ground segment becomes one of supervisory control and operations management, rather than detailed control of operations. Experience has shown that, generally, spacecraft have enough spares to meet mission life-time requirements, so additional redundant parts are not necessarily needed for ASM.

In the opinion of the study participants, the present system and current spacecraft operate quite well in that mission objectives and user data needs are satisfied. The present space segment, however, was designed to operate with man and his ground control function as an integral element. Successful space segment operation currently requires closure through the ground segment both before and after the occurrence of faults. ASM will remove this requirement from the day-to-day activities of space segment operations.

I. Conclusions

The following conclusions are those of the study group participants and result from analysis of the material developed during this study.

1. ASM would reduce the vulnerability problem. There is a need to decrease space segment dependence on the ground segment because the ground segment is vulnerable to both hostile action and operator error. By eliminating dependence on the ground segment for fault detection, isolation, and recovery management, and for routine operations functions such as power management and ephemeris updating, space system vulnerability will be significantly reduced.

2. The ASM capability need not impose operational constraints on the system user. If anything, the user should perceive a more responsive spacecraft with ASM present. New procedures for user system operations and data retrieval should not be required. Data outage resulting from most internal faults would be reduced from hours to seconds, making the ASM capability virtually transparent to the space segment data user.

3. ASM would require a change in the conduct of operations and control. The role of the ground segment in system operations must be redefined. Detailed control of routine operations and maintenance functions would be assumed by the space segment, with supervisory ground control. Supervisory control would be maintained by an audit trail capability that would provide nonreal-time (up to 6 months) visibility into maintenance actions, and by the capability for ground segment override of space segment autonomous actions.

4. ASM would add complexity to the spacecraft design; therefore, new methods for specifying, testing, and validating ASM-augmented spacecraft are needed. Concepts for specifying, testing, and validating ground-based, fault-tolerant processing systems have recently been developed. Interaction between computer and spacecraft technologists during this study has shown these concepts to be applicable to ASM. New methodologies for design and analysis are required to address such issues as fault coverage and recovery latency, measures of effectiveness, risk assessments, and proof-of-correctness.

5. A more effective means of transferring technology from research to applications programs would be required. The ASM study has served as a forum for the exchange of technology between researchers and application specialists. A continuation of information exchanges between these two communities will increase the level of awareness of both the technological problems and their potential solutions. As noted above in item 4, the collective experience of fault-tolerant data processing system specialists can serve as a surrogate for guiding the evolution of new spacecraft methods and new technologies required to satisfy space segment environmental constraints.

6. New technology developments would be required. Two specific technological developments were identified:

- (1) A highly reliable fault-tolerant computing capability with nonvolatile back-up memory to enable autonomous maintenance.
- (2) An autonomous navigation capability to enable independence of routine ground operations.

The fault-tolerant computing system is expected to have complete authority over spacecraft resources employed during reconfiguration by using hierarchical recovery management algorithms, diagnostic test procedures, fault-trail reporting mechanisms, and normal spacecraft operations. This authority must manage contention for system resources and manage subsystem interdependencies arising during anomalous operations. The conceptual design requirements for 60-day/6-month autonomy necessitates moving the navigation function from the ground to the spacecraft.

7. A strong corporate commitment to ASM by the Air Force would be required to make ASM successful. The implementation of ASM would be a phased program, with the spacecraft fleet evolving from non-ASM to ASM spacecraft over a period of several years. The spacecraft would not

instantly become totally autonomous. The pace of ASM development and implementation would depend upon the resources, technology, and chosen program applications that are provided. To plan the implementation of ASM and coordinate the actions of the System Program Offices and the ground segment, a strong, long-term corporate commitment would be needed. This would insure successful integration of ASM into the Air Force's space system.

8. Confidence in ASM must be instilled by creation of a systematic modeling, analysis, and demonstration program. Total confidence in ASM will result only after operations are proven to be predictable and understandable. However, proof-of-concept demonstrations of such individual ASM capabilities as battery reconditioning, autonomous recovery from bus undervoltage conditions, and autonomous computer self-diagnoses, will help provide early confidence in ASM. Confidence will be further established during the transition phase when quantitative figures of merit for ASM and non-ASM strategies can be developed within the flight environment.

9. ASM is a viable concept. ASM is the technological infusion of ground-based functions into long-lived, highly-reliable spacecraft. These functions are well understood and operating successfully on the ground now. Precepts borrowed from fault-tolerant computing will provide guidance for evaluation of fault-detection, isolation, and recovery techniques appropriate to the space environment. Other studies are in progress that will provide insight into the solution of the autonomous navigation problem, and no other technology gaps have been identified. Thus, ASM is workable and, given the urgency of the present situation, it should be started now.

II. Recommendation

The study group recognizes the need for ASM, and has found the technology available in today's spacecraft systems to be a good foundation from which to proceed to ASM. The plan presented is practicable; it aims at a series of prudent, gradually expanding (from subsystem to system level) capability demonstrations. The study group therefore recommends that the Air Force proceed with the technology development and research programs as outlined in the Implementation Plan and Research Agenda. These programs would provide the earliest possible demonstration of ASM as a valid system-level capability, and lay the research-oriented groundwork for the "second generation" ASM of the 1990s.

References

1. Toy, W. N., "Fault-Tolerant Design of Local ESS Processors," *Proceedings of the IEEE*, Vol. 66, No. 10, October 1978, pp. 1126-1145.
2. Katsuki, D., et al., "Pluribus - An Operational Fault-Tolerant Multiprocessor," *Proceedings of the IEEE*, Vol. 66, No. 10, October 1978, pp. 1146-1159.
3. Cooper, A. E., and Chow, W. T., "Development of On-board Space Computer Systems," *IBM Journal of Research and Development*, Vol. 20, No. 1, January 1976, pp. 5-19.
4. Gilley, G., "The Fault Tolerant Spaceborne Computer (FTSC)," *American Astronautical Society, Annual Rocky Mountain Guidance and Control Conference*, February 24-28, 1979.
5. Rennels, D. A., "Architectures for Fault-Tolerant Spacecraft Computers," *Proceedings of the IEEE*, Vol. 66, No. 10, October 1978, pp. 1255-1268.
6. Hopkins, A. L., Jr., et al., FTMP - A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft," *Proceedings of the IEEE*, Vol. 66 No. 10, October 1978, pp. 1221-1239.
7. Wensley, J. H., et al., "SIFT: The Design and Analysis of a Fault Tolerant Computer for Aircraft Control," *Proceedings of the IEEE*, Vol. 66, No. 10, October 1978, pp. 1240-1255.
8. Siewiorek, D. P., et al., "A Case Study of C.mmp, C.m*, and C.vmp: Part I - Experiences with Fault Tolerance in Multiprocessor Systems," *Proceedings of the IEEE*, Vol. 66, No. 10, October 1978, pp. 1178-1199.
9. Gault, J. W., Trivedi, K. S., Clary, J. B., "Validation Methods Research for Fault Tolerant Avionics and Control Systems - Working Group Meeting II," Conference Publication 2130, National Aeronautics and Space Administration, Washington, D.C., 1980.
10. *Thermoelectric Outer Planets Spacecraft (TOPS) Advanced System Technology Project Final Report*, Technical Memorandum 33-589, Jet Propulsion Laboratory, Pasadena, Calif., April 1, 1973.